**Vysoká škola báňská – Technická univerzita Ostrava**

**Fakulta bezpečnostního inženýrství**

**Katedra bezpečnostních služeb**

# Kybernetická ochrana v retailu

**Student: Tomáš Vlček**

**Vedoucí bakalářské práce: Ing. Vojtěch Jarkuliš**

**Supervizor bakalářské práce: doc. Mgr. Ing. Radomír Ščurek, Ph.D.**

**Studijní program: Požární ochrana a průmyslový bezpečnost**

**Studijní obor: Technická bezpečnost osob a majetku**

**Termín odevzdání bakalářské práce: 16. 4. 2021**

# Anotace

VLČEK, T. Kybernetická ochrana v retailu. Ostrava, 2021. 45 stran. Bakalářská práce. VŠB – TU Ostrava, Fakulta bezpečnostního inženýrství, Katedra bezpečnostních služeb. Vedoucí bakalářské práce Ing. Vojtěch Jarkuliš.

Tato bakalářská práce se zabývá kybernetickou ochranou v prostředí retailu. Úvodní část obsahuje výčet nejdůležitějších právních předpisů a technických norem souvisejících s oblastí kyberprostoru. Teoretická část je zaměřena na charakteristiku kybernetické bezpečnosti a kybernetických hrozeb. Shrnuje technické prostředky a technologie sloužící pro ochranu před kybernetickými útoky a charakterizuje jednotlivé procesy retailu. Praktická část je zaměřena na analýzu bezpečnostních rizik informačních systémů v retailu a následný návrh minimálních požadavků pro zajištění ochrany před kybernetickými útoky.

**Klíčová slova:** kybernetická ochrana, retail, kybernetický útok

# Summary

VLČEK, T. Cybersecurity in Retail. Ostrava, 2021. 45 pages. Bachelor Thesis. VŠB – TU Ostrava, Faculty of Safety Engineering, Department of Security Services. Supervisor Ing. Vojtěch Jarkuliš.

This bachelor thesis deals with cybersecurity in retail environment. The introductory part contains a list of the most important legal regulations and technical standards related to cyberspace. The theoretical part is focused on the characteristics of cyber security and cyber threats. Thesis summarizes the technical resources and technologies used to protect against cyber attacks and characterizes the individual retail processes. The practical part is focused on the analysis of security risks of information systems in retail and the proposal of minimum requirements to ensure protection against cyber attacks.

**Key words:** cybersecurity, retail, cyber attack.

# Obsah

# SEZNAM ZKRATEK

| | |
|---|---|
| TCP/IP | Přenosový protokol síťové vrstvy |
| CIA | Confidentiality, Integrity, Availability (důvěrnost, integrita, dostupnost), triáda informační bezpečnost |
| HDD | Hard Disk Drive (Pevný disk) |
| SSD | Solid-State Drive (Polovodičový disk) |
| IS/IT | Informační Systém a Technologie |
| POS systém | Pokladní a obchodní systém |
| NFC | Bezdrátová komunikace elektronických zařízení na krátkou vzdálenost |
| EMV | Celosvětový standard pro operace mezi čipovými kartami |
| ISMS | Systém řízení bezpečnosti informací |
| DoS | Denial of Service (odepření služby) |
| DDoS | Distributed Denial of Service (distribuované odepření služby) |
| XSS | Cross-Site Scripting (typ kybernetického útoku) |
| JQL | Java Query Language (dotazovací jazyk pro manipulaci s databází) |
| VPN | Virtuální soukromá síť |
| WI-FI | Wireless Fidelity (komunikační standard pro bezdrátový přenos dat) |
| PIN | Personal Identification Number (osobní identifikační číslo) |
| HTTP | Hypertext Transfer Protocol (internetový protokol pro komunikaci se servery) |
| HTTPS | Hypertext Transfer Protocol Secure (internetový protokol umožňující zabezpečenou komunikaci se servery) |
| TLS | Transport Layer Security (kryptografický protokol) |
| SSL | Secure Socket Layer (kryptografický protokol) |
| WPA | Wi-Fi Protected Access (chráněný přístup k Wi-Fi) |

# 1 ÚVOD

Práce s obrovským množstvím dat a citlivých informací je v dnešní době základním pilířem všech sfér společnosti, to jak vládních, vojenských, lékařských, finančních či podnikových. Neoprávněný přístup či únik soukromých dat by mohl vést k negativním nebo dokonce i destruktivním důsledkům a z toho důvodu získala kybernetická bezpečnost nejvyšší možnou prioritu. Kybernetická bezpečnost je disciplína, která se věnuje ochraně dat, informací a systémů používaných k jejich zpracování. S rostoucím objemem a propracovaností kybernetických útoků musí společnost stále držet krok a vytvářet vhodná opatření ke zlepšení ochrany a následného zamezení těmto typům útoků.

Cílem této práce je studie kybernetické ochrany a návrh minimálních požadavků pro zajištění ochrany před kybernetickými útoky se zaměřením na prostředí retailu.

Úvodní část práce se zabývá právními předpisy a technickými normami, které souvisí s problematikou oblasti kybernetické a informační bezpečnosti.

Čtvrtá kapitola definuje strukturu kyberprostoru včetně komplexního popisu jednotlivých vrstev, ze kterých je kyberprostor složen.

V páté kapitole je představena a definována kybernetická bezpečnost, která je doplněna o princip informační bezpečnosti. Kapitola shrnuje jednotlivé prvky tvořící základ informační bezpečnosti a rozebírá typy dat, informací a opatření používaných v podnicích.

Šestá kapitola se zabývá klasifikací kybernetických hrozeb a detailním popisem jednotlivých typů kybernetických útoků.

Sedmá kapitola se zaměřuje na deskripci procesů včetně charakteristiky podpůrných informačních systémů a technologií maloobchodu, konkrétně jde o front-office a back-office systémy. Další části kapitoly se věnují fungování elektronického obchodu a způsobům zabezpečení on-line transakcí.

V osmé kapitole jsou komplexně shrnuty jednotlivé technické prostředky a nástroje, které v současné době slouží jako bezpečnostní standard kybernetické ochrany.

V deváté kapitole jsou posouzena bezpečnostní rizika související s napadením informačního systému oblasti maloobchodu. Pro posouzení rizik je využito analytických metod FMEA a CARVER doplněných o Paretův princip. V poslední části kapitoly probíhá vzájemná komparace výsledků obou zpracovaných metod.

Závěrečná část práce se věnuje návrhu minimálních požadavků kybernetické ochrany se zaměřením na prostředí maloobchodu.

# 2 REŠERŠE LITERATURY

Během zpracování této bakalářské práce bylo čerpáno z několika odborných publikací, které souvisí s kybernetickou bezpečností a teorií retailu. Následuje jejich výčet a stručný popis.

**KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.**

Tato odborná publikace se komplexně zabývá oblastí kybernetické bezpečnosti, zejména charakteristikou kybernetického prostoru, principy informační bezpečnosti a základními druhy organizačních a technických opatření. Monografii jsem využil pro zpracování čtvrté a osmé kapitoly.

**ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk s.r.o., 2018. ISBN 978-80-7380-737-5.**

Tato monografie se v obecné a konkrétní rovině zabývá charakteristikou kybernetických útoků a obranou před nimi. Analyzuje slabiny informačních systémů a na konkrétních případech popisuje možnosti jejich minimalizace. Tato kniha byla hlavním podkladem
pro šestou kapitolu.

**SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.**

Tato publikace se zabývá problematikou pojetí bezpečnosti IS/IT – od právních předpisů, přes technické normy až po doporučené postupy a právní aspekty. V mé práci jsem čerpal z části legislativy kybernetické bezpečnosti.

**CIMLER, Petr. *Retail Management*. V Praze: Vysoká škola ekonomická, 2008. ISBN 978-80-245-1456-7.**

Tato kniha zprostředkovává základní teoretické koncepty a nástroje řízení maloobchodní firmy. Soustřeďuje se hlavně na procesy, tvorbu sortimentu, řízení pohybu zboží a také na organizaci podnikových procesů a řízení pracovníků. Knihu jsem využil pro zpracování 7. kapitoly.

# 3 PRÁVNÍ ÚPRAVA A NORMY OBLASTI KYBERNETICKÉ BEZPEČNOSTI

**Zákon č. 181/2014 Sb., o kybernetické bezpečnosti** a změně některých souvisejících zákonů je základem právní úpravy kybernetické bezpečnosti České republiky. Zákon upravuje práva a povinnosti osob, pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti a upravuje zajišťování bezpečnosti sítí informačních systémů a elektronických komunikací. Cílem zákona je stanovení základní úrovně bezpečnostních opatření, zlepšení detekce kybernetických bezpečnostních incidentů a zavedení systému opatření k reakci na tyto incidenty. Od roku 2014 došlo k několika novelizacím Zákona o kybernetické bezpečnosti, poslední a aktuální novelizace proběhla v únoru 2020.

**Vyhláška o kybernetické bezpečnosti č. 82/2018 S**b., zapracovává Směrnici NIS pro významné informační systémy a sítě elektronických komunikací využívané poskytovatelem digitálních služeb, upravuje obsah a strukturu bezpečnostních dokumentací, obsah a rozsah bezpečnostních opatření. Kategorizuje kybernetické bezpečnostní incidenty a náležitosti včetně způsobů jejich řešení.

**Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích** stanoví významné informační systémy a kritéria pro jejich určení. Významný informační systém je zde definován jako informační systém, jehož správcem je orgán veřejné moci. Systém je běžně využíván k zajištění: [4]

- elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci,
- kontrolní nebo inspekční činnosti a státního dozoru.

V roce 2020 došlo k novelizaci Vyhlášky č. 317/2014 Sb., s cílem upřesnit kritéria pro určení, zda je daný informační systém významný.

V roce 2016 byla vydána **Směrnice Evropského parlamentu a Rady (EU) 2016/1148** o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Evropské Unii (Směrnice NIS), která vznikla z důvodu zavedení jednotného standardu úrovně kybernetické bezpečnosti s cílem zlepšit fungování vnitřního trhu EU. Rozšiřující požadavky směrnice byly zapracovány do Zákona o kybernetické bezpečnosti prostřednictvím novelizace Zákona č. 205/2017 Sb. Některé z povinností uložené Směrnicí NIS již Zákon o kybernetické bezpečnosti upravoval, avšak došlo i k rozšíření oblastí

ochrany a prevence a to např. pro poskytovatele digitálních služeb, kdy je podstatný §2, který říká: „*Poskytovatel digitální služby je povinen zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informačních systémů, které využívá v souvislosti se zajišťováním své služby, přičemž tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy.“*

**Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR)** stanovuje pravidla ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů. Nařízení definuje osobní údaje jako jakékoliv informace o identifikovatelné nebo neidentifikovatelné fyzické osobě. Mezi osobní údaje patří např.: jméno, pohlaví, věk, datum narození, IP adresa, e-mailová adresa či telefonní číslo.

Vztažení GDPR pro kybernetickou bezpečnost: za využití všech přístupných technických a organizačních opatření je povinnost chránit osobní údaje a data před kompromitací. V případě narušení ochrany osobních dat vzniká nutnost ohlášení incidentu příslušnému úřadu (Úřad pro ochranu osobních údajů). [10]

**Směrnice Evropského parlamentu a Rady 2016/680** upravuje ochranu fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů.

**Zákon č. 110/2019 Sb., o zpracování osobních údajů** je adaptační zákon, který upřesňuje a dále upravuje podmínky zpracování osobních údajů v souladu se Směrnicí Evropského parlamentu a Rady 2016/680 a Nařízením Evropského parlamentu a Rady (EU) 2016/679 2016/679.

Informační bezpečnost je definována i řadou norem **ISO/IEC 27000.** Mezi základní normy informační bezpečnosti patří ČSN ISO/IEC 27001, kdy se jedná o mezinárodně platný standard, který podrobně popisuje požadavky na zavedení, implementaci, údržbu a neustálé zlepšování systému řízení bezpečnosti informací (ISMS), jehož cílem je pomoci organizacím zvýšit bezpečnost informačních aktiv. Norma ČSN ISO/IEC 27002 poskytuje doporučení osvědčených postupů a opatření v oblasti řízení bezpečnosti informací. Organizace splňující dané požadavky těchto norem mohou získat certifikaci ISO 27001.

# 4 KYBERPROSTOR

Kyberprostor může být definován jako virtuální počítačový svět, jež je tvořen prvky komunikačních a informačních technologií vytvářející celosvětovou globální počítačovou síť, která je základem veškeré on-line komunikace. Tato rozsáhlá globální síť je dále tvořena počítačovými systémy, které jsou do této sítě připojeny a které v ní interagují. Interakce uvedených systémů je závislá na zásahu jednotlivých uživatelů (administrátorů či koncových uživatelů). Propojení celého systému pak zajišťuje TCP/IP protokol, tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem. [2]

Kyberprostor je dynamický, neustále se měnící systém, který je zcela závislý na materiální podstatě, tedy technologiím umožňující existenci nehmotného média (kyberprostoru). Jednotlivé technologie, jmenovitě prvky sítí, počítačové systémy či cloudové úložiště zajišťují stabilitu a funkčnost, avšak kyberprostor je schopen se přizpůsobit a měnit se i při poškození hmotného média. V případě poškození či úplného zhroucení fyzického média (všech jeho částí) následuje nenávratné poškození, popřípadě zánik kyberprostoru. Hlavními vlastnostmi struktury kyberprostoru jsou interaktivita, otevřenost, globálnost, anonymita a bohatost na informace. Klíčovým elementem se stává zejména dostupnost a rychlost přenášených dat. [2]

## 4.1 Vrstvy kyberprostoru

Obvykle je kyberprostor považován za systém skládající se ze tří vrstev: [13]

- Fyzická
- Logická
- Sociální

Pojem fyzická vrstva představuje hmotné síťové komponenty (hardware), do kterých můžeme zahrnout veškerou infrastrukturu podporující síť (kabelovou, bezdrátovou a optickou) a fyzické konektory (vodiče, kabely, vysokofrekvenční zařízení, servery a počítače). [13]

Logická vrstva obsahuje logickou síťovou komponentu. Je obvykle chápána jako aplikační vrstva (protokoly, software) nebo informace (data). Jedná se o logické propojení mezi síťovými uzly, které představují všechna zařízení připojená k počítačové síti (počítače, mobilní telefony atd.). [46]

Sociální vrstva zahrnuje lidské a kognitivní aspekty a zahrnuje složku kybernetické osobnosti – „kyberosobnost“. Tato komponenta obsahuje identifikaci osoby na síti, a to pomocí e-mailové adresy, IP adresy počítače, čísla mobilního telefonu a dalších. Jednotlivec tedy může mít více kybernetických osobností (např. různé e-mailové účty). [13]

Vrstvy kyberprostoru lze také definovat podle dostupnosti a dohledatelnosti pro běžného uživatele. Podle uvedené definice si lze kyberprostor představit jako pomyslný ledovec, jehož viditelná část představuje prostor, ve kterém se uživatel běžně pohybuje. Jedná se o služby a data dostupná pomocí internetového prohlížeče. Avšak většinová sféra kyberprostoru je záměrně skryta, dostupná je pak pouze v rámci konkrétních sítí nebo zařízení. [2]

Popsané vrstvení lze rozdělit na následující tři části:

- Surface web
- Deep web
- Dark web

Surface web (povrchový internet) je ta vrstva, které je k dispozici většinové společnosti a lze se v ní „pohybovat“ za pomocí standardních prostředků (např. webové prohlížeče). Příkladem surface webu je např. Google, Facebook nebo internetové obchody. [12]

Deep web (hluboký internet) je vrstva, jejíž obsah není volně přístupný. Za formuláři chránící tuto vrstvu se ukrývá veškerý soukromý obsah uživatele, tj. např emailová pošta, online bankovnictví, profily na sociálních médií apod. Je tedy podmíněna zabezpečeným a autorizovaným přístupem. [13]

Dark web (temný internet) je vrstva, jejíž obsah je šifrovaný a přístupný pouze prostřednictvím speciálního softwaru. Není dohledatelný běžným internetovým vyhledávačem.

# 5 KYBERNETICKÁ BEZPEČNOST

Definovat kybernetickou bezpečnost není jednoduché, jelikož nemá jednotné obecně uznávané vyjádření. Při definování je tedy vhodné vycházet z již ustálených definic. Např. ve výkladovém slovníku pro kybernetickou bezpečnost je popsána jako: „*schopnost odolávat úmyslně i neúmyslně vyvolaným kybernetickým útokům a zmírňovat či napravovat jejich následky.*“ [27]

Oxford dictionary kybernetickou bezpečnost popisuje jako stav, při kterém je subjekt chráněn před kriminálním či neautorizovaným užitím elektronických dat. Patří sem i přijatá opatření k dosažení tohoto stavu. [30]

Ze zahraniční literatury lze použít definici Craigenovu a kol., kteří popisují kybernetickou bezpečnost jako organizaci a sběr zdrojů a procesů používaných k ochraně kyberprostoru před výskytem negativních událostí. [17]

Kybernetickou bezpečnost představuje sbírka nástrojů, zásad, bezpečnostních opatření a pokynů. Mimo jiné zde patří i postupy řízení rizik, školení, osvědčené postupy nebo záruky a technologie, které slouží k ochraně počítačové sítě a aktiv uživatele. Uživatelská aktiva zahrnují veškerá připojená výpočetní zařízení, personální infrastrukturu, aplikace, telekomunikační systémy a souhrn uložených informací v kybernetickém prostředí. Kybernetická bezpečnost se snaží o dosažení a udržení bezpečnostních podmínek, a chránit tak uživatelská aktiva před riziky v počítačové síti. [43]

Kybernetická ochrana je sektor výpočetní techniky známý jako informační bezpečnost, která je uplatňovaná u počítačů i sítí. Cílem informační bezpečnosti je ochrana před neoprávněným zacházením (úpravy, čtení, šíření, zničení), přičemž je důležité, aby informace zůstaly adekvátně přístupné a produktivní předpokládaným uživatelům. [28]

## 4.1 Princip informační bezpečnosti

Primárním zaměřením informační bezpečnosti je vyvážená ochrana důvěrnosti, integrity a dostupnosti dat (známá také jako triáda CIA). Tyto atributy jsou v literatuře označovány jako stavební kameny problematiky. V posledních letech se však uvažuje, zda je triáda CIA stále dostačující k řešení rychle měnících se technologických a obchodních požadavků. Z toho důvodu vznikají doporučení, která rozšiřují tyto základní atributy. Donn B. Parker navrhl tzn. Parkerian Hexad model, který znázorňuje sadu šesti prvků informační

bezpečnosti. Jedná se o tři klasické atributy triády CIA, doplněné o držení či kontrolu, autentičnost a užitečnost. Tyto atributy jsou „atomové“ v tom, že se nerozkládají na další složky a odkazují na jedinečné aspekty informací. Každé narušení bezpečnosti informací lze pak popsat jako ovlivnění jednoho či více z těchto základních atributů. [3]

Důvěrnost je pravděpodobně nejdůležitějším prvkem modelu CIA, je to vlastnost vztažena na informace, které nejsou zpřístupněna pro neoprávněné osoby, subjekty nebo procesy. Pokud jsou informace důvěrné, musí být zabezpečeny určitým způsobem. Každá organizace má nějakou formu citlivých informací, kde existuje pouze určitá skupina lidí s přístupem k nim. Pokud by došlo k úniku těchto informací, mělo by to škodlivé účinky na společnost či zákazníky. [38]

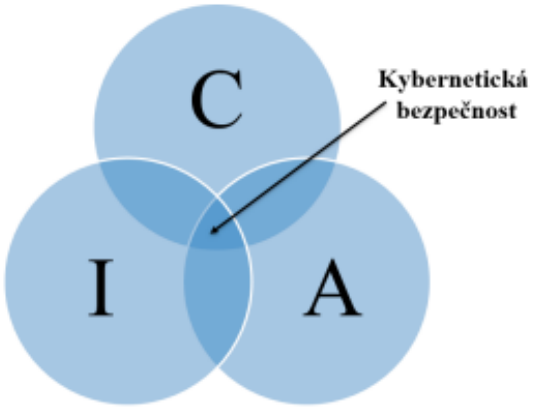
Integrita je definována jako schopnost předcházet neoprávněné nebo nežádoucí změně údajů. Tato definice není omezena pouze na neoprávněné vniknutí, ale zahrnuje i autorizovaný přístup k informačním aktivům. Je skutečností, že zaměstnanci jsou jedni z největších hrozeb integrity informací. Může se tak jednat například o neúmyslné smazání či vyplnění špatných dat. K zachování integrity je potřeba zavést nejen opatření k zabránění neoprávněným nebo nežádoucím změnám v datech, ale musí existovat i způsob, jak vrátit nebo obnovit tyto změny. [38]

Dostupnost je definována jako schopnost mít přístup k informaci, datům, nebo počítačovému systému v okamžiku potřeby. [2]

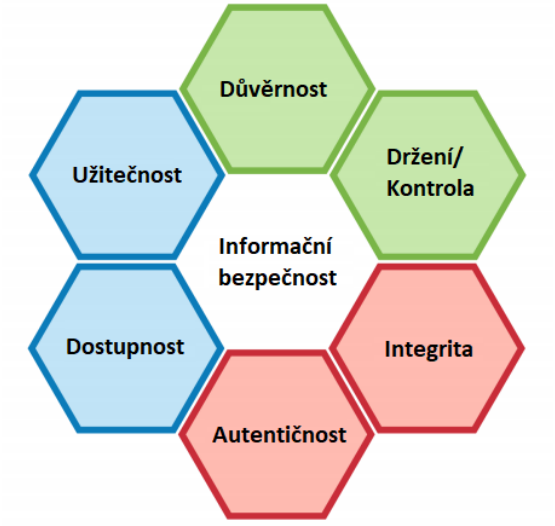
Atribut držení či kontroly je jedním z doplňků Parkera k modelu CIA. Tato součást mimo jiné řeší ochranu veřejných dat, která jsou vlastněna autorem. Jedná se např. o články, knihy, publikace zpráv atd. [38]

Autentičnost se týká ujištění, zda zpráva, transakce či jiná výměna informací pochází z předpokládaného zdroje. Autentičnost tedy zahrnuje metody, které kontrolují pravost druhé strany. Dnes je běžně používána metoda digitálního certifikátu. To jsou soubory, které potvrzují např. identitu společnosti, ke které přistupujeme prostřednictvím její webové stránky. [38]

Užitečnost je poslední základní složka Parkerian Hexadu. Často se přehlíží a z toho důvodu ji Parker komentuje: „*Užitečnost nelze přehlížet, je to zásadní součást tohoto modelu. Pokud data nejsou v užitečné formě, jsou nepoužitelné a v podstatě k ničemu.*“. [38]




*Obrázek č. 1: Triáda CIA a kybernetická bezpečnost [2]*




*Obrázek č. 2: Zobrazení Parker Hexadu [33], přeložil: autor*

## 4.2 Typy dat a informací v organizaci

Veškeré společnosti, bez ohledu na jejich velikost nebo odvětví působení, zpracovávají vlastní elektronické data a informace. Ty se zpravidla se ukládají na HDD, SSD disky počítačů, servery či cloudy, USB flash disky nebo optické disky jako CD, DVD. Zpracovávaná data a informace se ukládají v podobě souborů do adresářové struktury či databáze. Běžně jde o data a informace týkající se: [6]

- řízení lidských zdrojů:
    - osobní údaje o zaměstnancích (kontaktní informace, výše mzdy);
    - popis a obsazenost pracovních pozic;

- marketingu:
    - informace o klientech;
    - informace o dodavatelích;
    - detaily o obchodních vztazích;
    - informace o produktech či službách;
- managementu:
    - pracovní postupy;
    - bezpečnostní politika;
    - strategické plány;
- ICT:
    - síťová infrastruktura (nastavení, hesla);
    - systémy (nastavení, hesla);
    - aplikace (nastavení, hesla);
    - databáze (nastavení, hesla);
- finančního řízení:
    - výkazy;
    - účetní údaje;

## 4.3 Řízení informační bezpečnosti podniku

K řízení podnikové informační bezpečnosti lze přistoupit různými způsoby. Zpravidla se začíná jmenováním osoby, která bude za řízení informační bezpečnosti zodpovědná. Dále je třeba zavést základní bezpečnostní opatření organizační a technické povahy. Následně by mělo dojít k analýze rizik a návrhu organizačních a technických opatření včetně implementace. Tato opatření by měla být pravidelně přezkoumávána a vyhodnocována. Vhodné metodiky pro řízení informační bezpečnosti podniku jsou uvedeny v ISO/IEC 27001 a příslušná bezpečnostní opatření organizační a technické povahy v ISO/IEC 27002. Doporučení normy obsahuje 133 opatření, jež jsou rozděleny do 11 zásadních oblastí, které jsou nezbytné pro řízení celého systému. Tyto oblasti jsou následující: [8]

**Bezpečnostní politika:** Jedná se o pravidla a směrnice určující způsoby, jimiž jsou v dané organizaci řízena, chráněna a distribuována aktiva včetně citlivých informací. Bezpečnostní politika zajišťuje požadovanou úroveň důvěrnosti, integrity a autenticity dat informačního systému a zároveň zajišťuje ochranu transakcí v distribučním prostředí (internet). Bezpečnostní politika je postavena na zavedení a provozování systému řízení bezpečnosti informací (dále ISMS). [9]

**Organizace bezpečnosti informac**í: jde o infrastrukturu informační bezpečnosti, která se rozděluje na dvě základní skupiny: [9]

- interní organizace:
  - definuje role, které řídí bezpečnost informací;
- externí subjekty (organizace pro dodavatele a třetí strany):
  - vyhodnocení rizik při přístupu třetí strany k zařízením a službám IT;
  - vyhodnocení rizik při předání částí IT do provozu a správy jiné organizace;

**Řízení aktiv**: patří sem přiřazení odpovědnosti za aktiva, vedení evidence aktiv a klasifikace informací (tj. pravidla pro manipulaci s informacemi podle daného klasifikačního stupně).

**Bezpečnost lidských zdrojů** [9]

- Před vznikem pracovního vztahu – kritéria výběru pracovníků, závazky mlčenlivosti v pracovních smlouvách.
- Během pracovního vztahu – pravidelná bezpečnostní školení zaměstnanců, disciplinární řízení.
- Po změně nebo ukončení pracovního vztahu – vrácení prostředků IT, odebrání přístupových práv.

**Fyzická bezpečnost a bezpečnost prostředí:** zabezpečuje prostředí organizace a vytváří zóny s různými úrovněmi kontrol vstupu osob. Posuzuje: [9]

- zabezpečení perimetru;
- kontroly fyzického vstupu;
- zabezpečení místností a prostředků;
- veřejný přístup (recepce, nakládka a vykládka, vizuální kontroly);

Tato oblast se zaměřuje i na bezpečnost zařízení:

- umístění zařízení v odpovídajícím prostředí;
- zabezpečení dodávky energie;
- údržba zařízení;
- techniky mazání a likvidace paměťových médií (elektronická skartovačka, demagnetizace);

**Řízení komunikací a provozu IT řeší:** [9]

- provozní postupy a odpovědnosti:
  - dokumentace postupů, rozdělení povinností;
- řízení dodávek třetích stran;
- ochrana před škodlivými viry:
  - používání antivirových prostředků, pravidelná aktualizace ochranných prostředků;
- zálohování informací:
  - existence plánu zálohování, dodržování plánu zálohování;

- správa sítě:
    - správa vzdálených zařízení, ochrana důvěrnosti dat přenášených po síti;
- bezpečnost při zacházení s médii:
    - správa počítačových médií, bezpečnost systémové dokumentace;
- výměna informací,
    - výměna dat s jinými organizacemi, bezpečnost elektronické pošty;
- monitorování provozu:
    - pořizování auditních záznamů, monitorování používání IS;
- služby elektronického obchodu:
    - zabezpečení elektronického obchodu, on-line transakcí;

**Řízení přístupu uživatelů IS:** [9]

- politika řízení přístupu:
    - pravidla pro přidělování přístupových oprávnění;
- řízení přístupu uživatelů:
    - registrace uživatelů, evidence přidělených oprávnění, správa hesel;
- odpovědnosti uživatelů:
    - používání hesel, zásada prázdného stolu a prázdné obrazovky;
    - řízení přístupu uživatelů k síti;
    - řízení přístupu k operačnímu systému;
    - řízení přístupu k aplikacím;

**Akvizice, vývoj a údržba informačních systémů:** [9]

- bezpečnostní požadavky na systémy;
- bezpečnosti v aplikačních systémech;
    - validace vstupních dat, kontroly vnitřního zpracování, integrita zpráv;
- kryptografická opatření:
    - šifrování dat, digitální podpisy, správa klíčů;
- bezpečnost systémových souborů:
    - integrita souborů aplikace, testovací data, ochrana zdrojových kódů;

**Zvládání bezpečnostních incidentů:** [9]

- hlášení bezpečnostních incidentů (uživatelé):
    - způsob oznamování;
- zvládání bezpečnostních incidentů a náprav (ISMS odborníci);

**Řízení kontinuity činnosti organizace:** [9]

- strategie řízení kontinuity;
- plánování zálohování a bezproblémové obnovy (zálohovací servery);

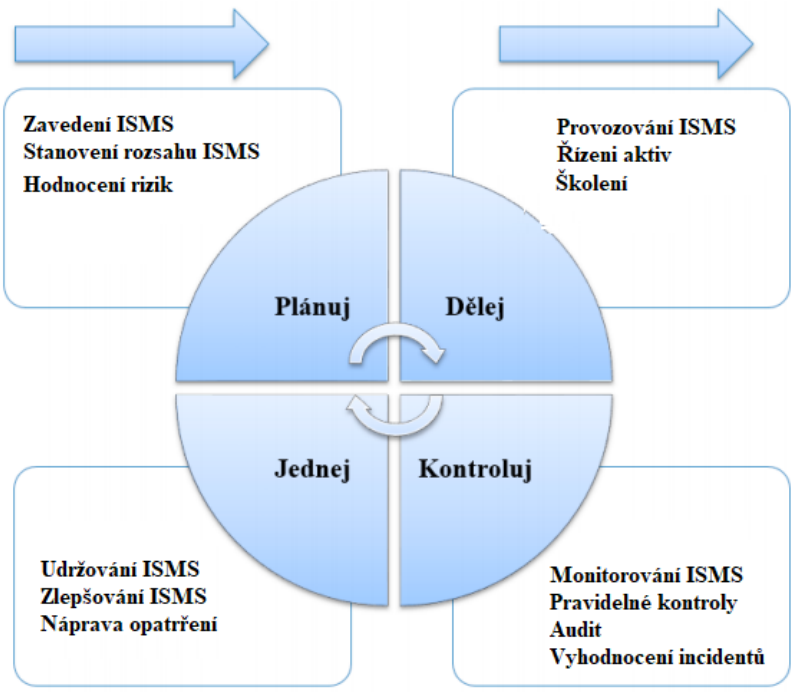
**Soulad s požadavky:** [9]

- shoda s právními požadavky.;

### 4.3.1 ISMS

Jedná se o systém strukturou určený normou ISO/IEC 27001. Poskytuje model ustavení, implementování, zpracovávání, monitorování, udržování a zlepšování ochrany informačních aktiv, aby byly dosaženy cíle organizace na základě posouzení rizik. [47]

Hlavním úkolem ISMS je provádět vhodná opatření za účelem potlačení či minimalizace hrozeb informační bezpečnosti. Zavedená opatření jsou poté s požadovanou úrovní záruk kontrolována. ISMS je řízen podle modelu PDCA (plánuj – dělej – kontroluj – jednej). Tento model může být použit na všechny procesy ISMS a znázorňuje principy nezbytné pro řízení bezpečnosti informačních systémů a sítí. [36]




*Obrázek č. 3: PDCA model aplikovaný na procesy ISMS [2], upravil: autor*

# 6 KYBERNETICKÉ HROZBY

Kybernetická hrozba je popisována jako škodlivý akt, jehož cílem může být poškození dat, krádež dat nebo získání neoprávněného přístupu do počítačové sítě či počítačového systému. Obecně se kybernetická hrozba dá popsat i jako pokus o změnu informace, aplikace či celého systému. [45]

## 6.1 Klasifikace kybernetických hrozeb

Možností klasifikace kybernetických hrozeb existuje celá řada, nejčastěji se člení podle: [2]

1) zdroje hrozby:
    - hrozby způsobené člověkem:
        - úmyslně (fyzické poškození systému, kybernetické útoky);
        - neúmyslně (omylem smazaná data);
    - technické chyby (chyba softwaru, hardwaru);
    - přírodní vlivy (povodně, požár);
2) zdroje působení:
    - hrozby vnitřní (zdroj hrozby je uvnitř organizace);
    - hrozby vnější (zdroj hrozby je vně organizace);
3) cíle hrozby
    - útok na triádu CIA;
    - útok na prvky kybernetické bezpečnosti (lidé, technologie, procesy);
4) motivace
    - je-li hrozba způsobena úmyslným jednáním člověka, lze se zabývat i jeho motivací k danému činu. Může jít například o hrozby:
        - za účelem finančního zisku;
        - za účelem konkurenční převahy;
        - za účelem odplaty;

## 6.2 Kybernetické útoky

Podle Cisco Systems lze kybernetický útok definovat jako: "*zákeřný a úmyslný pokus jednotlivce nebo organizace narušit informační systém jiného jednotlivce nebo organizace. Útočník obvykle hledá slabinu a snaží se ji využít ať už s cílem narušit dostupnost, důvěrnost nebo integritu dat.*" [14]

V dnešní době jsou kybernetické útoky čím dál tím častější a mají potenciál způsobit značnou škodu. Nebezpečnost těchto útoků pro společnost spočívá především v jejich asymetrii, kdy náklady na realizaci jsou zanedbatelné vzhledem ke škodě, kterou mohou způsobit. Hrozba a potenciál těchto útoků roste s počtem zařízení připojených k internetu, která mohou být napadena nebo ze kterých může být veden útok. [6]

Útok může být nabízen i jako služba včetně podpory, zpravidla je označován jako o tzv. CaS (Crime as Service). Jde o službu, pomocí které lze vyhledávat snadno napadnutelné systémy, rozesílat phishingové e-maily, nahrát na internet podvodnou aplikaci nebo shodit vybrané servery. [6]

Z pohledu firem a organizací se dnes již běžně používá připojení k internetu či informačním systémům, do kterých mají přístup zaměstnanci. Jedná se někdy i o přístupy ze svých soukromých zařízení. Firmy často využívající trendu – přístup do systému kdykoliv, odkudkoliv a z čehokoliv. To samozřejmě podporuje zvyšování rizika. [6]

Bezpečnostní návyky některých uživatelů jsou prakticky nulové, což představuje potenciální riziko. Příkladem mohou být hesla. Přestože požadavky na jejich délku a komplexitu jsou již běžnou věcí, z každoročních úniků databází hesel je zřejmé, že uživatelé používají stále snadno prolomitelná hesla (typu 123456). Dalším podobným bezpečnostním problémem může být např. sdílení informací na internetu. [6]

Taktéž vzdálenosti mezi obětí a útočníkem se stále prodlužují a při dnešní snaze co nejvíce činností automatizovat, riziko napadení roste. Kybernetický útok cílený původně na jen jeden systém se přelévá i do dalších systémů díky jejich propojení a sdílených zdrojů. Tradiční bezpečnostní řešení mnohdy selhávají a kybernetických útoků, jak malých, středních nebo velkých stále přibývá. Každá firma bez ohledu na velikost a předmět podnikání se může stát cílem útoku. Takový útok může přijít naprosto nečekaně nejen zvenku, ale i zevnitř, a proto by měla každá společnost přijmout alespoň základní bezpečnostní opatření organizační a technické povahy, která jí zpravidla nic nestojí anebo jsou náklady na jejich zavedení (s porovnáním možného dopadu) minimální. Kybernetické útoky nemusí být ani složité či cílené, avšak nechráněné organizace se mohou stát jednou z mnoha obětí. Většina takových útoků totiž probíhá tak, že útočník skenuje internet a hledá známou slabinu, které by se dalo využít, popřípadě rozešle obrovské množství podvodných emailů, a následně už jen čeká na potencionální oběť. Stručně řečeno, pokud jde o bezpečnost stále platí, že zaměstnanci jsou tím nejslabším článkem. [6]

## 6.3 Typy kybernetických útoků

Kybernetické útoky, jakožto útočné akce zaměřené na počítačové informační systémy a infrastruktury, počítačové sítě nebo zařízení osobních počítačů, dělíme do kategorií podle použitých metod útoku a charakteristiky dopadu. Nejčastěji jde o tyto typy kybernetických útoků:

### 6.3.1 Sociální inženýrství

Sociální inženýrství je termín používaný pro širokou škálu škodlivých činností využívající lidské chyby k získání soukromých informací, přístupu nebo cenností. V počítačové kriminalitě mají tyto kybernetické podvody lákat nic netušící uživatele k odhalení dat, šíření malwarových infekcí nebo zpřístupnění omezených systémů. Pachatel nejprve shromažďuje nezbytné základní informace, jako jsou potenciální vstupní body a slabé bezpečnostní protokoly potřebné k pokračování útoku. Dále míří na nedostatek znalostí uživatele skrze získání si důvěry a následně využívá akce, která může vést k odhalení citlivých informací nebo neoprávněnému přístupu ke kritickým zdrojům. [26]

**Techniky sociálního inženýrství:**

**Baiting**: u této techniky se útočníci snaží poskytnout něco, co oběti považují za užitečné. Může se jednat o předpokládanou aktualizaci softwaru nebo o USB disk obsahující cenná data, avšak ve skutečnosti se jedná o infikovaný soubor nebo malware. [22]

**Pretexting**: útočníci při využití této techniky vytváří falešnou identitu a používají ji k manipulaci svých obětí s cílem získat soukromé informace. Útočník může například předstírat, že je externím poskytovatelem IT služeb a vyžadovat podrobnosti o účtu oběti jako jsou hesla, e-mail apod. [22]

**Phishing**: Jedná se o nejběžnější typ útoku sociálního inženýrství. Phishingové podvodné e-mailové a textové zprávy jsou zaměřené na vytváření pocitu naléhavosti, zvědavosti nebo strachu obětí. Cílem útočníka je přimět oběť odhalit své citlivé informace, kliknout na odkaz vedoucí na škodlivé webové stránky nebo otevírat přílohy, které obsahují malware. [26]

**Whaling:** jde o phishing zaměřený na konkrétního, předem vybraného jednotlivce. Většinou se jedná o určitého výkonného nebo vlivného jedince např. organizace. Na rozdíl od běžného phishingu jsou tyto útoky více propracované a je třeba více úsilí na provedení, avšak negativní dopad může být mnohem větší.

### 6.3.2 Malware

Malware je termín používaný k popisu škodlivého nežádoucího softwaru, který byl vyvinut kybernetickými útočníky s cílem způsobit poškození dat, systémů nebo získat neoprávněný přístup k síti. Malware narušuje systémy prostřednictvím chyby v zabezpečení, šíří se různými způsoby od phishnigových e-mailů, infikovaných příloh či aplikací až po nezabezpečené webové servery. [34]

**Typy malwaru:**

**Virus**: jedná se o nejběžnější typ malwaru. Obvykle se šíří prostřednictvím infikovaných webových serverů, sdílení souborů nebo stahování e-mailových příloh. Je nečinný do chvíle, dokud není aktivován uživatelem. Jakmile k tomu dojde, dokáže se sám šířit skrze jiné programy a soubory. [23]

**Červy**: pojmenovány podle toho, jakým způsobem infikují systémy. Počínaje jedním infikovaným zařízením se dokážou proplétat sítí a infikovat tak další zařízení. Tento typ malwaru může velmi rychle napadnout celé sítě. [23]

**Spyware**: jak už název napovídá, je navržen tak, aby sledoval, co uživatel dělá. Tento typ malwaru funguje skrytě na pozadí počítače, kde pozoruje činnosti uživatele a shromažďuje informace. Může jít např. o údaje kreditních karet, hesla a další citlivé informace. [23]

**Ransomware**: malwarový program, který dokáže šifrovat data a procesy. Následně požaduje od oběti výkupné za obnovení přístupu v podobě kryptoměny. Ransomware bývá často mířený tak, aby ochromil nemocnice, policejní oddělení, maloobchodní společnosti nebo dokonce i celá města. Z důvodu velikosti těchto cílů dnes dochází k obrovskému nárůstu ransomware útoků. [23]

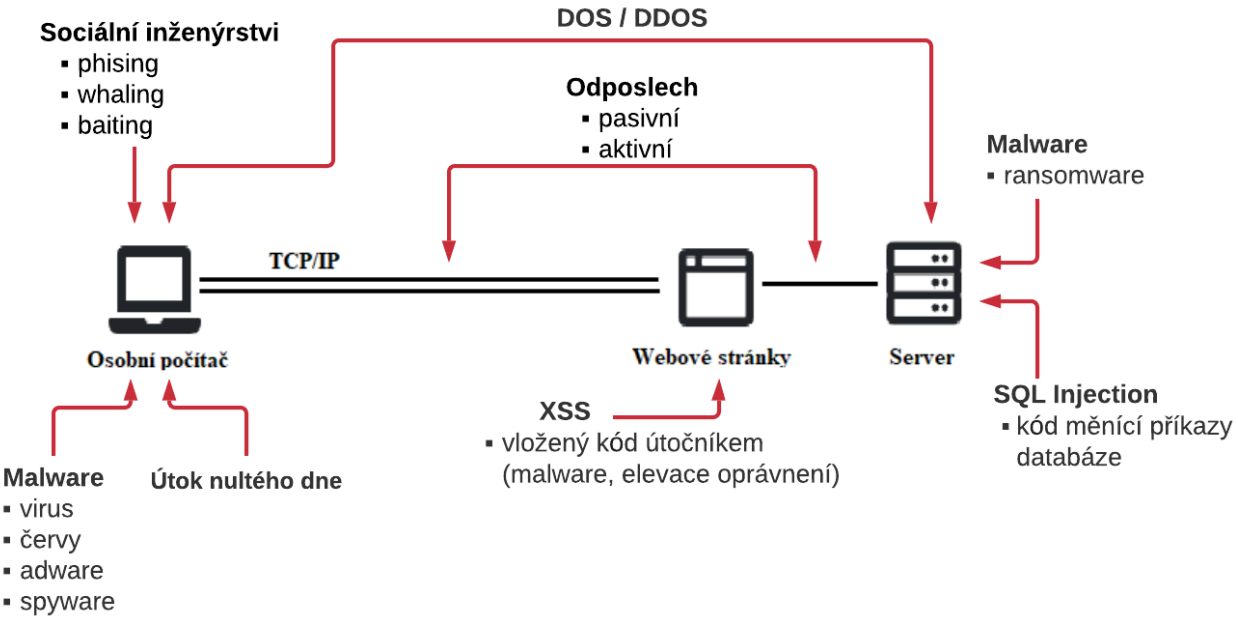
### 6.3.3 Další typy kybernetických útoků

**Útok odposlouchávaním:** dochází k nim prostřednictvím zachycení síťového provozu. Odposlechem může útočník získat hesla, čísla kreditních karet a další důvěrné informace, které by uživatel mohl posílat po síti. Odposlech může být aktivní nebo pasivní. [34]

- Pasivní odposlech – útočník detekuje informace „naslouchánim“ nešifrovaného přenosu zpráv pomocí specializovaného softwaru. [42]
- Aktivní odposlech – útočník aktivně získává informace tím, že se vydává za legitimní osobu např. při proniknutí do interní sítě pomocí malwaru. [42]

**Denial of service (DoS):** v českém překladu – odepření služby. Jedná se o útoky zaměřené na služby nebo servery, jejichž cílem je službu znefunkčnit a znepřístupnit ostatním uživatelům. Častým způsobem provedení tohoto útoku je přehlcení cíle požadavky. Podtypem útoku DoS je tzv. **distributed denial of service (DDoS)**, při kterém je pro přehlcení cílové služby požadavky využito velké množství rozptýlených počítačů. K přehlcení často dochází bez vědomí majitelů těchto počítačů, důvodem je předchozí infikování těchto systémů příslušným malwarem. Přehlcení požadavky může mít formu zaplavení provozu sítě náhodnými daty, které zabraňují protékání skutečných dat, což může způsobit neobvyklé zpomalení, nedostupnost služeb či pád celého operačního systému. [21]

**Útok nultého dne:** je v informatice označení útoku nebo hrozby, který se v počítači či systému snaží využít zranitelnosti používaných softwarů. Zákeřnost je v tom, že míří na chyby, které ještě nejsou obecně známy, resp. pro ně neexistuje ochrana (např. formou aktualizace systému či konkrétního softwaru). Označení nultého dne zde neoznačuje počet dní, ale skutečnost, že systém podléhá ohrožení až do vydání opravy. Doba ohrožení útokem nultého dne může být v rozmezí několika dnů, týdnů nebo roků, tzn. že doba jeho trvání je plně v rukou autorů vadného softwaru. [25]




*Obrázek č. 4: Typy kybernetických útoků [autor]*

V **příloze č. 1** se nachází výčet několika kybernetických incidentů za poslední roky.

# 7 RETAIL

Retail neboli maloobchod je podnik nebo činnost zahrnující nákup od velkoobchodu či od výrobce a jeho prodej bez dalšího zpracování konečnému spotřebiteli. Maloobchod vytváří vhodné seskupení zboží jakožto prodejní sortiment, zajišťuje pohotovou prodejní zásobu, poskytuje informace o zboží, vytváří vhodnou formu prodeje a předává marketingové informace dodavatelům. Maloobchodní činnost může probíhat v různých formách, které lze kombinovat a modifikovat. Obecně se maloobchod dělí na potravinářský a nepotravinářský. [1]

V potravinářském typu se obchoduje převážně s potravinami, avšak do sortimentu patří i např. čistící a prací prostředky, prostředky osobní hygieny či cigarety. Tento typ je pak nejvíce koncentrován, často s nejmodernějšími informačními a logistickými systémy. Důvodem jsou velké procházející objemy zboží, zájem o hromadné nákupy a pravidelnost odběru. [1]

Nepotravinářský maloobchodní prodej představuje širokou škálu sortimentu a druhů prodejen. Nepotravinářský maloobchod se neustále vyvíjí a vytvářejí se nové provozní typy s novými sortimenty. Může se jednat o sortiment pro volný čas, výpočetní techniky či prodej automobilů. [1]

Dále existují členění jako maloobchod specializovaný a univerzální, kdy užší sortiment (specializovaný) je spíše typický pro menší prodejny. Z hlediska místa, kde se nákup a prodej uskutečňuje, lze maloobchod rozdělit na: [1]

- Maloobchod realizovaný v síti prodejen (store retail)
    - Základní složkou jsou prodejní jednotky – prodejny. Může se jednat o obchodní dům nebo také o tržnice či zvláštní formy jako např. stánkový prodej.
- Maloobchod realizovaný mimo síť prodejen (non store retail)
    - Hlavními formami jsou:
        - prodejní automaty;
        - zásilkový obchod;
        - elektronicky – internetový obchod;

## 7.1 Proces maloobchodu

Proces maloobchodu je výsledkem mnoha specializovaných oblastí činností. Hlavní část procesu je však zabezpečována samotnými maloobchodníky. [40]

Proces maloobchodu se skládá z těchto činností: [40]

- Nákup a skladování zboží;
- Prodej a podpora prodeje zboží;
- Přeprava zboží (logistika);
- Finanční operace;
- Určení dodavatelů;
- Převzetí podnikatelského rizika;
- Ochrana osob a majetku;

## 7.2 Informační systémy v maloobchodě

Informační systémy a technologie (dále jen IS/IT) jsou nedílnou součástí provozu jakéhokoli podnikatelského subjektu. Pro maloobchodní podnikání, distribuci a logistiku je IS/IT nutnou podmínkou efektivní podpory klíčových procesů. V oblasti maloobchodu to znamená především optimalizaci všech procesů dodavatelsko-odběratelského řetězce. Z pohledu podniku jde o co nejvýhodnější nákupní podmínky, co nejnižší náklady na vnější i vnitřní logistiku, tj. optimalizace toků zboží mezi distribučními sklady a jednotlivými obchodními jednotkami či pohybu zboží na konkrétní jednotce. [1]

**Front-office procesy, tj.** procesy na obchodní jednotce, kde dochází k přímému kontaktu se zákazníkem. Z pohledu informačních technologií do této oblasti patří:

Pokladní a obchodní systémy neboli systémy inteligentních pokladen, které můžou být realizovány specializovaným hardwarem nebo na bázi standardních PC, včetně snímačů čárových kódu, terminálů pro platební karty, různých typů displejů apod. Mimo jiné sem patří i doplňkové systémy jako váhové systémy, etiketovací systémy, price checkery (zařízení pro kontrolu ceny) a další. [1]

Veškerý front-office hardware je realizován specializovaným softwarovým řešením, tzv. pokladním systémem. Na tento software jsou z pohledu maloobchodních procesů kladeny nároky na rychlost, jednoduchost ovládání a bezpečnost pokladních operací. [1]

**Back-office procesy:** jde o procesy realizované v pozadí prodejní jednotky, běžně jde o centrálu maloobchodní firmy či kanceláře prodejní jednotky. Zabezpečují podporu těch činností, které se bezprostředně nedotýkají koncového zákazníka na prodejně, avšak významným způsobem ovlivňují podmínky fungování prodeje: [1]

a) řízení obchodních jednotek, určující podmínky a pravidla řízení pohybu zásob zboží na prodejně, podmínky samotného prodeje zboží, cenové strategie nebo podporu prodeje pomocí marketingových akcí.
b) podmínky pro optimalizaci či automatizaci zásobování na prodejně, do této oblasti patří provozní vyhodnocování informací o zboží a na základě těchto informací jsou pak realizovány procesy nákupu, zásobování prodejních jednotek a logistické procesy ve skladech či na prodejnách. Jedná se např. o zajištění sortimentu.

V oblasti back-office se tedy odehrává podstatná část provozních procesů, kdy se na jejich realizaci používá specializovaný software. [1]

Vzhledem k obrovským objemům dat, nárokům na rychlost a kvalitu zpracování, okamžitou dostupnost centrálních dat z různých lokalit a potřebu využívat informace z různých manažerských úrovní je podpora těchto procesů bez využití IS/IT dnes už nemožná. [1]

### 7.2.1 Front-office: Pokladní a obchodní systém

Pokladní a obchodní systém (dále POS systém) je síť zařízení, která je určena k prodeji fyzického zboží maloobchodu. Síť se skládá jak z hardwarových, tak ze softwarových prvků, dohromady tvořící systém používaný k provedení transakcí a fakturací. [39][39]

Pro pochopení fungování POS zařízení je srozumitelnější přirovnání jej spíše k PC, jelikož funguje na podobném principu. Software je totiž nainstalován na hardwaru podobně jako u PC a je poháněn místním serverem nebo připojením k internetu. [39]

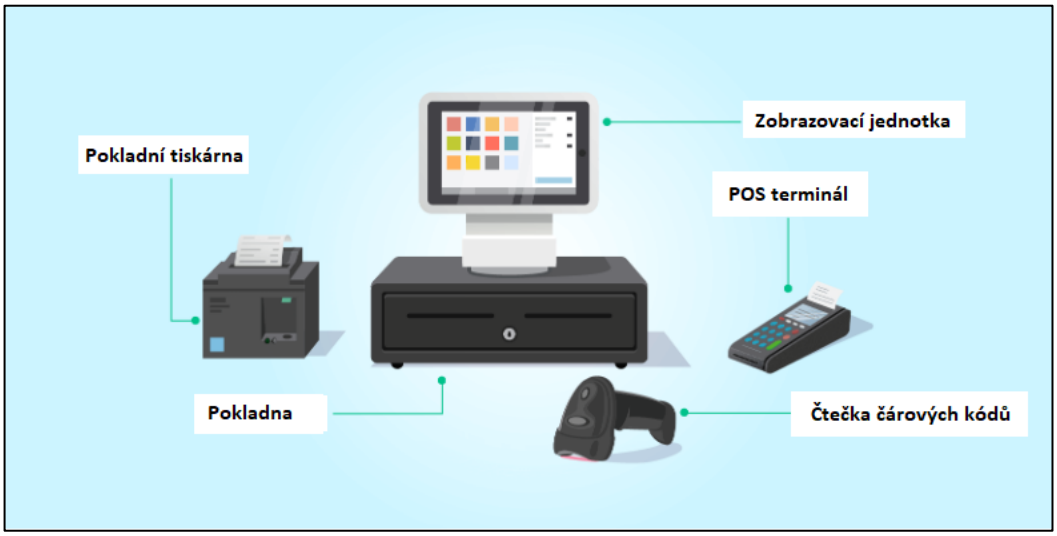
Samotný hardware je obvykle složen ze zobrazovací jednotky (monitor, tablet), klávesnice nebo dotykové obrazovky pro výběr produktu či zadávání dat, dále čtečky čárových kódů pro skenování účtovaných předmětů, tiskárny pro vytištění účtenky, registrační pokladny pro uložení hotovosti a terminálu pro přijímání platebních karet. [41]

Software nainstalovaný na POS zařízení, podobně jako u PC se systémy Windows nebo Mac slouží jako operační systém celého zařízení. V softwarovém rozhraní POS technologie lze zadávat data o produktech, které jsou určeny k prodeji nebo také provádět finanční transakce. Rozsah funkcí záleží na dostupném vybavení komponentů hardwaru. Mnoho maloobchodních podniků používá software, který byl vytvořen přímo na míru pro jejich konkrétní potřeby. [39]

U starších typů POS zařízení jsou veškerý software a data uloženy na místních serverech podniku. U větších maloobchodních podniků se dnes už však běžně používá cloudový systém POS. Veškerá data jsou u tohoto typu uložena na vzdáleném serveru (neboli „cloudu“). Tento typ umožňuje vzdálený přístup a správu systému přes internet. Výhoda cloudového typu je také v pravidelné aktualizaci systému, což je důležité pro bezpečnost dat. [39]

POS terminál, tj. čtecí elektronické zařízení, které umožňuje provedení bezhotovostní transakce platební kartou. Terminály jsou zpravidla integrovány do POS softwaru z důvodu bezproblémové správy a rychlosti řešení objednávek a transakcí. Bývají často opatřeny tiskárnou k vytištění dokladu o provedené transakci. [41]

POS terminály obvykle detekují všechny způsoby plateb, od karet založených na EMV čipech, po detekci NFC či bezkontaktní karty a dalších platebních možností, jako jsou Apple Pay, Google Pay apod. [41]




*Obrázek č. 5: Hardware prvky POS systému [41], přeložil: autor*

**Samoobslužná pokladna** je technologie, pomocí které maloobchodníci umožňují zákazníkům zpracovávat vlastní nákupy. Jsou tedy alternativou tradiční pokladny obsluhovanou zaměstnancem. Samotný zákazník provádí práci pokladníka sám, a to skenováním čárových kódů položek, popř. vybíráním produktu z dotykového displeje a následnou platbou za položky vložením hotovosti do stroje nebo bezkontaktní platbou.

Kromě skenování čárových kódů, samoobslužné pokladny mají funkci kontrolního vážení, kdy je pozorována hmotnost produktu a srovnávána s očekávanou. Zákazníkovi je pak umožněna další interakce jen v případě shody těchto hmotností.

Obvykle se i zde nachází zaměstnanec dohlížející na skupinu samoobslužných pokladen, který v případě potřeby pomáhá zákazníkům a kontroluje celý průběh.

Samoobslužné pokladny disponují přizpůsobeným softwarem pro jednoduchou a bezpečnou interakci zákazníkem. Integrovány jsou do místní sítě či na cloud podobně jako u tradičních POS pokladen.

**Scan&Shop** je další možností samoobslužného zpracování nákupu. Jde o systém využívající přenosný snímač čárových kódů, který zákazník používá ke skenování produktů při nakupování. Po skončení nákupu zákazník vygeneruje ukončovací kód skeneru a pomocí pokladního snímače jej přenese do dané pokladny (POS zařízení), kde jsou staženy informace o čárových kódech. Platba poté probíhá klasickým způsobem. [49]

Samoobslužné nakupování Scan&Shop doplnila i možnost skenovat produkty pomocí mobilní aplikace určené k danému obchodu. Jedná se tedy o oblíbenou alternativu ke skenerům, která ještě více usnadní a zrychlí nákup. Přenesení informací o nákupu do pokladny a samotná platba funguje stejně jako u přenosných snímačů.

### 7.2.2 Back-office software

Maloobchodní software pro back-office se používá ke správě obchodních operací, které nesouvisejí s přímým prodejem zboží. Obchodní procesy řízené back-office softwarem obvykle zahrnují určitou kombinaci řízení zásob, správy účetnictví, výroby a řízení dodavatelského řetězce. Softwarová řešení pro back-office se vyvinula s nástupem cloudu jako služby pro maloobchodníky. Poskytovatelé back-office softwaru nabízí cloudové služby, které zjednodušují a zefektivňují funkce správy back-office, a to zejména pro rozsáhlé společnosti. Cloudové služby poskytují maloobchodníkům alternativu pro řízení těchto procesů pomocí outsourcingu, kdy je předána správa systému back-office externímu poskytovateli. [44]

Cloudové řešení back-office systému poskytuje nezbytné funkce pro celkovou správu z jediného webového rozhraní. Mnoho softwarových platforem pro back-office jsou přístupné z jak z mobilních, tak i stolních zařízení a jsou navzájem kompatibilní. Mezi nejběžnější funkce back-office softwaru patří: [44]

- správa zásobování a inventury;
- správa POS systému;
- správa účetnictví;

- podpora prodeje, věrnostního programu;
- elektronická výměna dat;
- zpracování faktur;
- obchodní zprávy;
- monitorování klíčových ukazatelů výkonu;

## 7.3 Online obchod

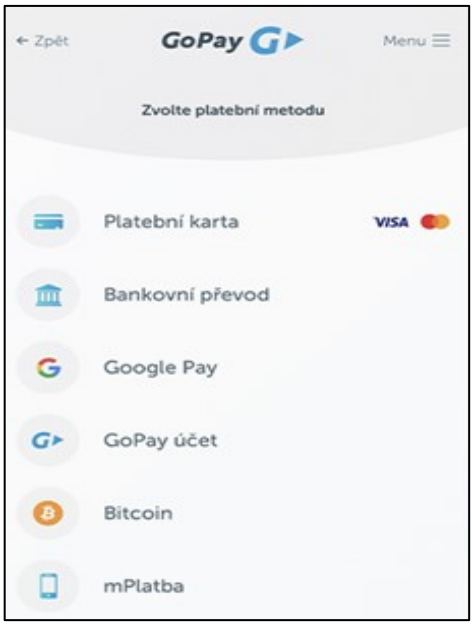
Internetový obchod (e-shop) je forma elektronického obchodu, která spotřebitelům umožňuje nakupovat maloobchodní zboží přes internet pomocí webového prohlížeče nebo mobilní aplikace. Typický internetový obchod umožňuje zákazníkovi procházet katalog produktů, vyhledávat zboží podle parametrů nebo podle shody s názvem. Jednotlivé produkty obsahují zpravidla detailní stránku s podrobnějším popisem, specifikacemi, obrázky a samozřejmě cenou.

E-shop je většinou realizován pomocí sady skriptů, které spolupracují s databází, v níž jsou detaily o zboží uloženy. Sofistikovanější e-shopy dokážou spolupracovat i s ekonomickým, účetnickým nebo logistickým softwarem, který daná firma používá (většinou pomocí datových souborů v dohodnutém formátu). [35]

### 7.3.1 Platební metody

Pro zřizování e-shopu je třeba zajistit několik důležitých funkcí, kterými musí každý web nebo aplikace disponovat. Nejzásadnější funkcí je výběr způsobu transakce a jejího provedení. Provedení transakce může být řešeno fyzicky (dobírka) nebo on-line (s využitím platební brány). On-line platby v České republice jsou uskutečňovány prostřednictvím: [24]

- platebních karet;
- bankovních převodů;
- on-line platebních tlačítek;
- mobilních plateb;
- elektronických peněženek (Google Pay, PayPal);
- plateb v kryptoměně (Bitcoin);




*Obrázek č. 6: Platební metody GoPay [autor]*

### 7.3.2 Platební brány

Z technického hlediska je online platební brána aplikační software, který umožňuje obchodníkovi přijímat on-line platby od zákazníků. Platební brána dokáže prostřednictvím poskytovatele platebních služeb (např. banky, GoPay) bezpečně ověřit zadané údaje o zákazníkovi, a zjistit, zda jsou k dispozici potřebné finanční prostředky na vykonání transakce. Platební brány dokážou zpracovávat různé platební metody, jako jsou elektronické peněženky, platební karty, nebo nově platby v podobě kryptoměny, a to vše z jednoho rozhraní. [18]

Vzhledem k tomu, že dochází k zpracování velmi citlivých informací, jako jsou údaje držitelů karet, je bezpečnostní aspekt nanejvýš důležitý. Proto jsou veškeré citlivé údaje šifrovány a zajištěny pro bezpečné předávání. Jinými slovy, platební brána funguje jako prostředník mezi zákazníkem a obchodníkem a zajišťuje, že transakce proběhne bezpečně a rychle. [18]

Platební brána může být poskytována samotnou bankou nebo může být zajišťována specializovaným poskytovatelem finančních služeb. [18]


*Obrázek č. 7: Platební brána GoPay [autor]*

Následující přehledová tabulka uvádí některé ze zástupců největších maloobchodních on-line obchodů zaměřených na potraviny a módu v České republice, včetně zabezpečení jejich webových stránek kryptografickými certifikáty (viz kapitola č. 8) a způsobů zabezpečení provádění plateb skrze internetové platební brány.

*Tabulka č. 1: Přehled retailových on-line obchodů [autor]*

| Maloobchod | Šifrování webových stránek | Platební brána | Zabezpečení platební brány |
|---|---|---|---|
| Rohlik.cz | SSL | ČSOB | 3D Secure[1], SSL[2] |
| Kosik.cz | SSL | ČSOB | 3D Secure, SSL |
| Z-market.cz | Nezabezpečeno | - | - |
| Zalando.cz | SSL | Go Pay | 3D Secure, SSL |

### 7.3.3 Struktura a způsob fungování on-line obchodu

Základem on-line obchodu je kombinace čtyř systémů: [48][48]

- webový server, který se stará o chod webových stránek a webových aplikací;
- databázový systém, který vykonává kontrolu a správu všech položek uložených ve skladu (probíhá neustálá aktualizace při objednávání zboží, bývá zpravidla napojen na systém objednání zásob);
- obchodní systém, jež zpracovává finanční operace;
- skladový systém propojený s expedicí;

Příklad fungování plně elektronického systému on-line obchodu včetně schématu je uveden **v příloze č. 2.**

[1] 3D Secure – zabezpečení informací o kartě zákazníka (např. číslo karty)
[2] SSL – šifrovací protokol

# 8 TECHNICKÉ PROSTŘEDKY KYBERNETICKÉ BEZPEČNOSTI

Technické prostředky představují základní prvky bezpečnostních opatření. Primárně se věnují pravidlům pro nastavení informačních a komunikačních systémů a služeb. Následující výčet kategorií opatření odpovídá některým cílům technických opatření podle Zákona o kybernetické bezpečnosti, Vyhlášky o kybernetické bezpečnosti a normy ISO/IEC 27002.

**Nástroje pro ochranu integrity komunikačních sítí**

Správce a provozovatel informačního systému kritické informační infrastruktury by měl: [2]

- vytvořit vhodné navržení topologie sítě včetně segmentace sítě organizace, tzn. rozdělit síť do samostatných zón, které lze samostatně řídit, sledovat a chránit;
- zajistit řízení bezpečnosti přístupu a komunikace v rámci vnějších a vnitřních sítí;
- pomocí kryptografie (šifrování) zajistit důvěrnost a integritu dat při vzdáleném přístupu, správě komunikační sítě nebo při přístupu pomocí bezdrátových technologií (např. VPN, Wi-Fi);
- aktivně blokovat nežádoucí komunikaci (spam filtry);
- pro segmentaci sítě využívat takové síťové prvky, které garantují vysokou míru zabezpečení (routery, switche);

**Nástroje pro ověřování identity uživatelů**

Podle § 19 Vyhlášky o kybernetické bezpečnosti musí povinná osoba zabezpečit aplikační, informační a komunikační systémy nástrojem pro ověření identity uživatelů. Tento nástroj je dnes již běžně součástí všech operačních systémů (Linux, Windows, iOS). Je potřeba aby vykonával: [2]

- ověření identity osoby (před zahájením aktivit v informačních, aplikačních nebo komunikačních systémech);
- řízení počtu možných neúspěšných pokusů o přihlášení;
- opětovné ověření identity po dané době nečinnosti;
- centralizovanou správu identit;

Pro ověřování identit uživatelů může povinná osoba využívat například i autentizační mechanismus, který není založený pouze na identifikátoru účtu a heslu. Využívá totiž vícefaktorové autentizace s nejméně dvěma rozdílnými faktory, kdy kromě běžných přihlašovacích údajů (1. faktor) může vyžadovat např. PIN či softwarový token, což je aplikace chytrého telefonu, spárovaná s autentizačním serverem, který generuje unikátní klíč potřebný k přihlášení. [2]

**Nástroje pro řízení přístupových oprávnění**

Jedná se o nástroje umožňující centralizovanou správu uživatelského přístupu k některým z aktiv (tj. soubory, aplikace, adresáře), nebo správu oprávnění k činnostem jako jsou čtení a zápis dat. [2]

**Nástroje pro ochranu před škodlivým kódem**

Jsou to nástroje zajišťující nepřetržitou automatickou kontrolu serverů, mobilních zařízení, datových úložišť, komunikačních sítí a prvků komunikační sítě. Monitorují také používání výměnných zařízení a datových nosičů. Tyto nástroje musí procházet pravidelnou aktualizací, aby bylo dovršeno nejvyšší možné míry bezpečnosti. Příkladem může být anti-malware, anti-virus, firewall, anti-spam, NetFlow a další. [2]

**Nástroje pro zaznamenávání činnosti uživatelů významných informačních systémů**

Jedná se o nástroje pro kontrolu (audit) logů, které slouží k zaznamenávání bezpečnostních a provozních událostí, jejichž uchovávání slouží jako podklad pro případné vyšetřování kybernetických bezpečnostních incidentů. Z toho důvodu zajišťují: [37]

- jednoznačnou síťovou identifikaci zařízení uživatele,
- sběr informací o bezpečnostních a provozních událostech, tj.:
    - datum a čas, typ činnosti, úspěšnost nebo neúspěšnost činnosti, využitá aktiva;
    - ochranu takto získaných informací před neoprávněným čtením či jejich změnou;
- přístup pověřených osob k auditu logů, správnost dokumentování a četnost kontrol;

**Nástroje pro detekci kybernetických bezpečnostních incidentů**

Správce nebo provozovatel sítě musí používat nástroje pro detekci kybernetických bezpečnostních událostí, které slouží pro ověření a kontrolu přenášených dat v rámci vnitřní

komunikační sítě, včetně kontroly přenášených dat z vnější komunikační sítě. Zároveň zajišťuje blokování nežádoucí komunikace. K detekci kybernetických bezpečnostních událostí lze využívat výstupů mnoha softwarových nástrojů, např. firewall, systémy pro detekci narušení (IDS), anti-virus, anti-malware, anti-DDoS nebo VPN. [2]

**Aplikační bezpečnost**

Tato kategorie bezpečnosti je přímo zaměřena na aplikace, které jsou využívané v informačních systémech, ať už v rámci počítačového systému, mobilního zařízení nebo webové aplikace. Je běžně zabezpečována firewally a testována pomocí tzv. penetračních testů. [2]

Smyslem firewallu je zabránit nežádoucí síťové komunikaci mezi různými sítěmi nebo rozhraní sítě a koncovým počítačovým systémem. Jedná se kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Existuje celá řada druhů firewallů, dělí se podle způsobu fungování, způsobu nasazení nebo umístění. [19]

Penetrační testy jsou metody zaměřené na identifikaci zranitelností, které by mohly být přítomny v informačním systému, síti nebo aplikaci. Jsou prováděny kvalifikovanými experty, kteří využívají technik skutečných útočníků. Jejich cílem je odhalit slabiny a způsoby proniknutí, tím následně poskytují návody pro zlepšení bezpečnosti a snížení existujícího rizika. [29]

**Kryptografické prostředky**

Za účelem zajištění důvěrnosti a integrity dat je nutné využití kryptografie (šifrování). Jedná se o matematickou operaci, pomocí které jsou převedeny informace z podoby srozumitelné do podoby nesrozumitelné. Tím se zajišťuje, že osoba, která k nim získá neoprávněný přístup, se s nimi nebude moci seznámit a modifikovat je. Pro rozšifrování dané informace je potřeba kryptografického klíče. [2]

Podle § 26 Vyhlášky o Kybernetické bezpečnosti musí povinná osoba pro ochranu aktiv informačního a komunikačního systému: [11]

- používat aktuálně odolné a správně nakonfigurované kryptografické algoritmy a kryptografické klíče;
- využívat systému správy klíčů a certifikátu, který zajišťuje generování, distribuci, ukládání a změny těchto klíčů;
- prosazovat bezpečné nakládání s kryptografickými prostředky;

Užití kryptografických metod v praxi je dnes již nepostradatelnou částí kybernetické bezpečnosti. Používají se například pro zašifrování osobních údajů v internetovém prohlížeči, pro šifrování disku počítače nebo e-mailových zpráv. Šifrování podléhají i cloudové systémy a úložiště, pro které se data nejprve transformují pomocí šifrovacích algoritmů a až poté se umisťují do těchto úložišť. Zde je však třeba seznámit uživatele či zákazníky využívající cloudových služeb se zásadami a postupy poskytovatele, a to v rámci způsobu šifrování a správy šifrovacích klíčů. [31]

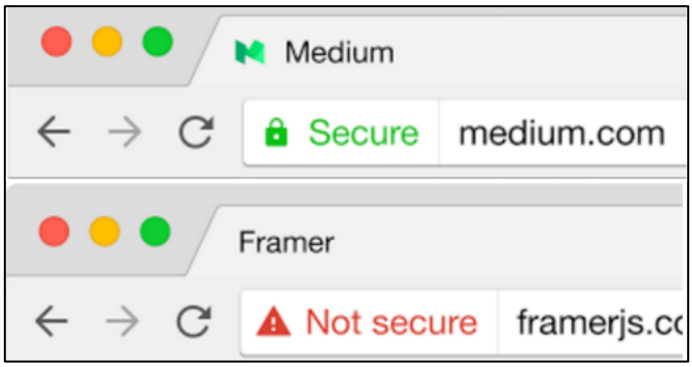
**Kryptografie webových serverů**

HTTP je v informatice protokol, který je používán pro komunikaci mezi webovým prohlížečem a webovým serverem. Pro zvýšení bezpečnosti přenosu dat mezi těmito subjekty se využívá protokolu HTTPS, který doplňuje protokol HTTP o šifrovací protokol TLS (někdy označován jako SSL). [15]

Za účelem zajištění vysokého stupně ochrany soukromí, šifruje protokol TLS data, která jsou přenášena během komunikace se serverem. V praxi to znamená, že kdokoli se pokusí zachytit přenášená data, uvidí pouze nečitelnou kombinaci znaků, jež je téměř nemožné dešifrovat. TLS dále zahájí proces – tzv. handshake, pomocí kterého si obě komunikující strany vymění potřebná data. Výsledkem výměny je vzájemné ověření a vytvoření klíčních relací pro šifrovací algoritmy. Metoda handshake je základní součástí fungování HTTPS. [16]

Zabezpečení HTTPS se doporučuje tam, kde jsou vyžadovány přihlašovací údaje nebo platební údaje uživatele, příkladem mohou být platební brány elektronických obchodů.

Od roku 2016 moderní webové prohlížeče jako je Google Chrome implementoval funkci, označující webové servery využívající protokolu HTTPS jako zabezpečené. [16]




*Obrázek č. 8: Označení přítomnosti protokolu HTTPS [15]*

# 9 POSOUZENÍ RIZIK OBLASTI MALOOBCHODU

Posuzování rizik lze označit za proces, který je nezbytný pro určení nejvýznamnějších rizik vybraného objektu. Výstupní data procesu posouzení rizik jsou základem pro tvorbu opatření minimalizující nepřijatelná rizika na přijatelnou úroveň. Riziko ovšem není možné zcela eliminovat, lze jej pouze snížit, přenést na jiný subjekt, například pojišťovnu nebo riziko akceptovat. Proces posouzení tvoří tři hlavní po sobě jdoucí fáze, jedná se o identifikaci, analýzu a hodnocení rizik. Kromě již zmíněných jednotlivých fází řízení rizik existují i další, které utváří kompletní systém. Systém posuzování rizik vyplývá z normy ČSN EN 31010 – Management rizik – Techniky posuzování rizik. Následující podkapitoly se zaměřují pouze na zmíněné tři hlavní fáze procesu:

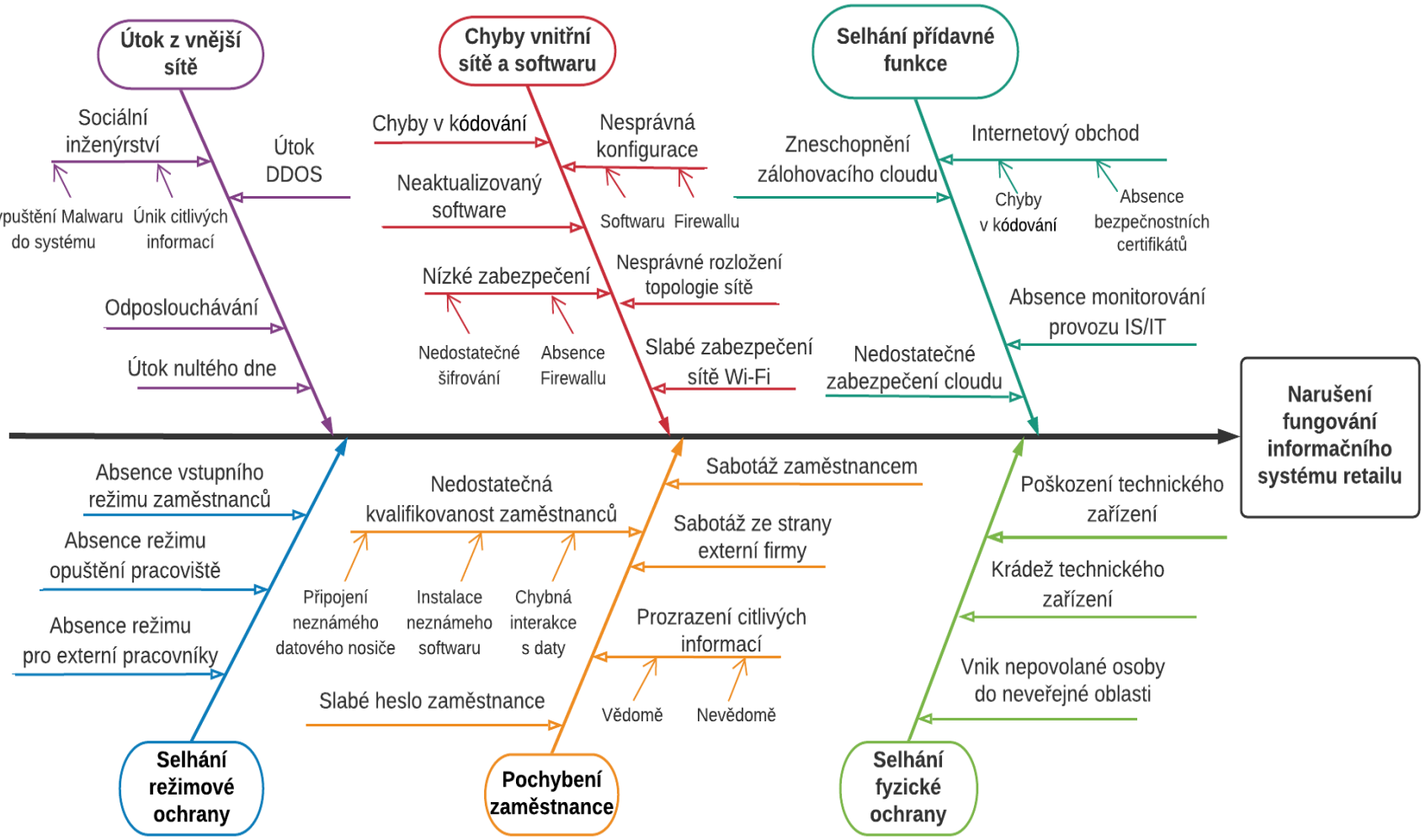
## 9.1 Identifikace rizik

Analytická metoda Ishikawův diagram, zvaná též jako diagram příčin a následků či diagram rybí kosti, je určena pro grafické modelování příčin vzniku rizik. Zakladatelem této metody je japonský univerzitní profesor a významný průkopník v oblasti řízení rizik Kaoru Ishikawa. Principem diagramu je hledání co nejvíce možných příčin pro stanovený následek či problém, který hrozí. Při sestavování diagramu je vhodné využití brainstormingu více zainteresovaných osob. V první fázi metody se stanoví následek, který je umístěn v „hlavě kostry“ a poté jsou k němu připsány kategorie příčin, které se dále rozvětvují na jednotlivé dílčí příčiny. [32]

Vstupním následkem pro zpracovaný Ishikawův diagram je narušení fungování informačního systému retailu. Pro definování výstupů bylo určeno šest hlavních kategorií příčin:

- Útok z vnější sítě
- Chyby vnitřní sítě a softwaru
- Selhání přídavné funkce
- Selhání režimové ochrany
- Pochybení zaměstnance
- Selhání fyzické ochrany

Kompletní zpracování Ishikawova diagramu je zobrazeno na obr č. 9.




*Obrázek č. 9: Ishikawův diagram [autor]*

## 9.2 Analýza rizik metodou FMEA

Analýza selhání a jejich dopadů (označována jako FMEA), je analytická kvantitativní metoda sloužící k identifikaci poruch systému, jejich příčin a důsledků. Účelem metody FMEA je nalézt ty příčiny, které vykazují nejvyšší míru rizikovosti a následně navrhnout taková opatření, která tato rizika sníží. [7]

Pro hodnocení metody FMEA slouží hodnotící parametry P, N a H, které jsou zaneseny do tabulky č. 2. Jejich vzájemným součinem se vypočítá výsledná rizikovost, kterou představuje písmeno R viz vzorec (1). Platí zde přímá úměra, čím vyšší je výsledná rizikovost R, tím vyšší je i nepřijatelnost. [7]

**R** se počítá podle následujícího vzorce:

$$\boldsymbol{R = P \times N \times H} \qquad (1)$$

**R** – výsledná míra rizika

**P** – pravděpodobnost vzniku rizika

**N** – závažnost následků

**H** – odhalitelnost rizika

*Tabulka č. 2: Parametry metody FMEA [5]*

| R | Výsledná míra rizika | P | Pravděpodobnost vzniku rizika |
|---|---|---|---|
| 0-3 | bezvýznamné riziko | 1 | velice nepravděpodobná |
| 4-10 | akceptovatelné riziko | 2 | spíše nepravděpodobná |
| 11-50 | mírné riziko | 3 | pravděpodobná |
| 51-100 | nežádoucí riziko | 4 | velmi pravděpodobná |
| 101-125 | nepřijatelné riziko | 5 | trvalá hrozba |
| **N** | **Závažnost následků** | **H** | **Odhalitelnost** |
| 1 | zanedbatelná | 1 | odhalitelné v době jeho spáchání |
| 2 | malá | 2 | odhalitelné během první hodiny |
| 3 | střední | 3 | odhalitelné do jednoho dne |
| 4 | vysoká | 4 | nesnadno odhalitelné |
| 5 | velmi vysoká | 5 | neodhalitelné |

Pro zkonstruování metody FMEA využiji již vymodelované příčiny rizik z Ishikawova diagramu. Tyto vstupní data budou jednotlivě zanesena do tabulky č. 3,4 a doplněna o hodnoty z tabulky č.2.

*Tabulka č. 3: Provedení metody FMEA [autor]*

| Číslo | Kategorie identifikovaného rizika | Identifikované riziko | P | N | H | R | Relativní četnost R |
|---|---|---|---|---|---|---|---|
| 1 | Útok z vnější sítě | Sociální inženýrství – infikování sítě maloobchodu malwarem | 5 | 5 | 4 | 100 | 11,90 |
| 2 | | Sociální inženýrství – únik citlivých informací | 5 | 4 | 4 | 80 | 9,52 |
| 3 | | Útok nultého dne | 2 | 4 | 4 | 32 | 3,81 |
| 4 | | Útok DDOS | 5 | 3 | 2 | 30 | 3,57 |
| 5 | | Odposlouchávání | 1 | 4 | 4 | 16 | 1,90 |
| 6 | Chyby vnitřní sítě a softwaru (back office, POS) | Chyby v kódování softwaru | 1 | 4 | 4 | 16 | 1,90 |
| 7 | | Nesprávná konfigurace softwaru | 2 | 3 | 4 | 24 | 2,86 |
| 8 | | Nízké zabezpečení z důvodu absence firewallu | 2 | 5 | 3 | 30 | 3,57 |
| 9 | | Neaktualizovaný software | 5 | 4 | 2 | 40 | 4,76 |
| 10 | | Nesprávné rozložení topologie sítě | 1 | 3 | 4 | 12 | 1,43 |
| 11 | | Slabé zabezpečení sítě Wi-Fi | 3 | 4 | 4 | 48 | 5,71 |
| 12 | Selhání přídavné funkce | Chyba v kódování e-shopu | 1 | 3 | 4 | 12 | 1,43 |
| 13 | | Absence bezpečnostních certifikátů e-shopu | 2 | 4 | 4 | 32 | 3,81 |
| 14 | | Nedostatečné zabezpečení cloudu maloobchodního systému | 2 | 5 | 4 | 40 | 4,76 |
| 15 | | Zneschopnění zálohovacího cloudu maloobchodu | 2 | 3 | 3 | 18 | 2,14 |
| 16 | | Absence monitorování provozu IS/IT | 3 | 3 | 3 | 27 | 3,21 |

*Tabulka č. 4: Provedení metody FMEA pokračování [autor]*

| Číslo | Kategorie identifikovaného rizika | Identifikované riziko | P | N | H | R | Relativní četnost R |
|---|---|---|---|---|---|---|---|
| 17 | Selhání režimové ochrany | Absence / porušení vstupního režimu zaměstnanců | 3 | 2 | 1 | 6 | 0,71 |
| 18 | | Absence /porušení režimu opuštění pracoviště | 4 | 4 | 1 | 16 | 1,90 |
| 19 | | Absence / porušení režimu výkonu práce pro externí pracovníky | 2 | 2 | 2 | 8 | 0,95 |
| 20 | Pochybení zaměstnance | Sabotáž zaměstnancem | 2 | 4 | 2 | 16 | 1,90 |
| 21 | | Sabotáž ze strany externí firmy | 2 | 3 | 2 | 12 | 1,43 |
| 22 | | Vědomé prozrazení citlivých informací | 2 | 4 | 4 | 32 | 3,81 |
| 23 | | Nevědomé prozrazení citlivých informací | 3 | 3 | 4 | 36 | 4,29 |
| 24 | | Slabé heslo zaměstnance | 4 | 3 | 5 | 60 | 7,14 |
| 25 | | Nedostatečná kvalifikovanost zaměstnance – chybná interakce s daty či zařízením | 4 | 2 | 2 | 16 | 1,90 |
| 26 | | Nedostatečná kvalifikovanost zaměstnance – instalace neznámého softwaru | 3 | 4 | 3 | 36 | 4,29 |
| 27 | | Nedostatečná kvalifikovanost zaměstnance – připojení neznámého datového nosiče | 2 | 4 | 3 | 24 | 2,86 |
| 28 | Selhání fyzické ochrany (prodejny) | Poškození technického zařízení | 3 | 2 | 1 | 6 | 0,71 |
| 29 | | Krádež technického zařízení | 3 | 2 | 1 | 6 | 0,71 |
| 30 | | Vnik nepovolané osoby do neveřejné oblasti (kanceláře) | 3 | 3 | 1 | 9 | 1,07 |

Metoda FMEA je doplněna o Paretovu analýzu využívající Paretova principu 80/20, tzn. že je nutné minimalizovat alespoň 80 % ze všech rizik, aby bylo dosaženo dostatečného zabezpečení. Pro zobrazení rozmezí 80 % nejzávažnějších rizik je využito Lorenzovy křivky. Zobrazení Paretova diagramu je uvedeno **v příloze č. 3.**

Z výsledků Paretova diagramu pro metodu FMEA tedy vyplývá, že mezi 80 % nejzávažnějších rizik patří riziko č. 1, 2, 24, 11, 9, 14, 23, 26, 3, 13, 22, 4, 8, 16, 27, 7.

## 9.3 Analytická metoda CARVER

Analytická metoda CARVER byla vyvinuta americkou armádou pro posuzování vojenských cílů. Díky možnosti hodnocení rizik z pohledu útočníka se postupem času tato metoda stala vhodnou i pro rámec fyzické bezpečnosti. K posuzování identifikovaných rizik metoda CARVER využívá šest hodnotících parametrů. Těmito parametry jsou: [20]

- C = Criticality = důležitost, kritičnost
- A = Accessibility = přístupnost
- $R_1$ = Recuperability = obnovitelnost
- V = Vulnerability = zranitelnost
- E = Effect on population = vliv na společnost
- $R_2$ = Recognizability = rozpoznatelnost

Jednotlivé parametry obsahují bodové ohodnocení (1-5) včetně popisných kritérií. Vzájemný součet hodnot parametrů znázorňuje výslednou míru daného rizika R.

$$\boldsymbol{R = C + A + R_1 + V + E + R_2} \quad (2)$$

Při použití metody CARVER vycházím z identifikovaných rizik pomocí Ishikawova diagramu. Kompletní výčet hodnotících parametrů je uveden **v příloze č. 4**. Tabulky č. 5 a 6 uvádějí posuzovaná rizika včetně veškerého hodnocení dle principu metody.

*Tabulka č. 5: Provedení metody CARVER [autor]*

| Číslo | Kategorie identifikovaného rizika | Identifikované riziko | C | A | $R_1$ | V | E | $R_2$ | R | Četnost R |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Útok z vnější sítě | Sociální inženýrství – infikování sítě maloobchodu malwarem | 5 | 5 | 4 | 5 | 5 | 5 | 24 | 4,90 |
| 2 | | Sociální inženýrství – únik citlivých informací | 4 | 4 | 3 | 5 | 5 | 5 | 21 | 4,29 |
| 3 | | Útok nultého dne | 4 | 2 | 4 | 2 | 3 | 1 | 15 | 3,06 |
| 4 | | Útok DDOS | 3 | 5 | 2 | 5 | 5 | 5 | 20 | 4,08 |
| 5 | | Odposlouchávání | 3 | 2 | 4 | 2 | 4 | 1 | 15 | 3,06 |
| 6 | Chyby vnitřní sítě a softwaru (back office, POS) | Chyby v kódování softwaru | 4 | 2 | 3 | 2 | 2 | 1 | 13 | 2,65 |
| 7 | | Nesprávná konfigurace softwaru | 3 | 2 | 3 | 3 | 3 | 1 | 14 | 2,86 |
| 8 | | Nízké zabezpečení z důvodu absence firewallu | 5 | 4 | 4 | 5 | 5 | 4 | 23 | 4,69 |
| 9 | | Neaktualizovaný software | 4 | 2 | 1 | 3 | 4 | 3 | 14 | 2,86 |
| 10 | | Nesprávné rozložení topologie sítě | 3 | 1 | 5 | 1 | 2 | 1 | 12 | 2,45 |
| 11 | | Slabé zabezpečení sítě Wi-Fi | 3 | 4 | 3 | 3 | 4 | 4 | 17 | 3,47 |
| 12 | Selhání přídavné funkce | Chyba v kódování e-shopu | 3 | 4 | 2 | 4 | 4 | 4 | 17 | 3,47 |
| 13 | | Absence bezpečnostních certifikátů e-shopu | 5 | 4 | 3 | 4 | 5 | 4 | 21 | 4,29 |
| 14 | | Nedostatečné zabezpečení cloudu maloobchodního systému | 5 | 2 | 3 | 1 | 5 | 1 | 16 | 3,27 |
| 15 | | Zneschopnění zálohovacího cloudu maloobchodu | 3 | 2 | 3 | 1 | 4 | 1 | 13 | 2,65 |
| 16 | | Absence monitorování provozu IS/IT | 4 | 3 | 3 | 3 | 1 | 3 | 14 | 2,86 |

*Tabulka č. 6: Provedení metody CARVER pokračování [autor]*

| Číslo | Kategorie identifikovaného rizika | Identifikované riziko | C | A | $R_1$ | V | E | $R_2$ | R | Četnost R |
|---|---|---|---|---|---|---|---|---|---|---|
| 17 | Selhání režimové ochrany | Absence / porušení vstupního režimu zaměstnanců | 2 | 4 | 1 | 5 | 3 | 4 | 15 | 3,06 |
| 18 | | Absence /porušení režimu opuštění pracoviště | 4 | 4 | 1 | 5 | 1 | 3 | 15 | 3,06 |
| 19 | | Absence / porušení režimu výkonu práce pro externí pracovníky | 2 | 3 | 1 | 4 | 1 | 3 | 11 | 2,24 |
| 20 | Pochybení zaměstnance | Sabotáž zaměstnancem | 4 | 4 | 3 | 5 | 3 | 5 | 19 | 3,88 |
| 21 | | Sabotáž ze strany externí firmy | 3 | 3 | 2 | 4 | 3 | 4 | 15 | 3,06 |
| 22 | | Vědomé prozrazení citlivých informací | 4 | 5 | 3 | 5 | 1 | 5 | 18 | 3,67 |
| 23 | | Nevědomé prozrazení citlivých informací | 3 | 4 | 3 | 4 | 1 | 4 | 15 | 3,06 |
| 24 | | Slabé heslo zaměstnance | 4 | 3 | 1 | 5 | 3 | 3 | 16 | 3,27 |
| 25 | | Nedostatečná kvalifikovanost zaměstnance – chybná interakce s daty či zařízením | 2 | 3 | 1 | 3 | 3 | 3 | 12 | 2,45 |
| 26 | | Nedostatečná kvalifikovanost zaměstnance – instalace neznámého softwaru | 4 | 4 | 3 | 4 | 2 | 4 | 17 | 3,47 |
| 27 | | Nedostatečná kvalifikovanost zaměstnance – připojení neznámého datového nosiče | 4 | 3 | 3 | 4 | 2 | 4 | 16 | 3,27 |
| 28 | Selhání fyzické ochrany (prodejny) | Poškození technického zařízení | 2 | 4 | 3 | 4 | 5 | 5 | 18 | 3,67 |
| 29 | | Krádež technického zařízení | 2 | 4 | 3 | 4 | 5 | 4 | 18 | 3,67 |
| 30 | | Vnik nepovolané osoby do neveřejné oblasti (kanceláře) | 3 | 5 | 1 | 4 | 3 | 4 | 16 | 3,27 |

Na výstupní hodnoty metody CARVER je aplikován Paretův princip 80/20 pomocí Paretova diagramu a Lorenzova křivky. Paretův diagram výsledků metody CARVER je uveden **v příloze č. 5.**

Z výsledků Paretova diagramu pro metodu CARVER tedy vyplývá, že mezi 80 % nejzávažnějších rizik patří riziko č. 1, 8, 2, 13, 4, 20, 22, 28, 29, 11, 12, 26, 14, 27, 30, 24, 5, 3, 23, 17, 21, 18.

## 9.5 Vyhodnocení rizik

V této kapitole jsou vzájemně srovnány výstupy metod FMEA a CARVER. Na základně vyhodnocení těchto výstupů viz tabulky č. 7 a 8 jsou mezi významná bezpečnostní a nepřijatelná rizika zařazena následující:

- sociální inženýrství – infikování sítě maloobchodu malwarem, sociální inženýrství – únik citlivých informací, útok nultého dne, útok DDOS, nízké zabezpečení z důvodu absence firewallu, slabé zabezpečení sítě Wi-Fi, absence bezpečnostních certifikátů e-shopu, nedostatečné zabezpečení cloudu maloobchodního systému, vědomé prozrazení citlivých informací, nevědomé prozrazení citlivých informací, slabé heslo zaměstnance, nedostatečná kvalifikovanost zaměstnance – instalace neznámého softwaru, nedostatečná kvalifikovanost zaměstnance – připojení neznámého datového nosiče.

*Tabulka č. 7: Komparační tabulka identifikovaných rizik [autor]*

| Číslo rizika | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FMEA | X | X | X | X | | | X | X | X | | X | | X | X | |
| CARVER | X | X | X | X | X | | | X | | | X | X | X | X | |
| **Vyhodnocení** | X | X | X | X | | | | X | | | X | | X | X | |

*Tabulka č. 8: Komparační tabulka identifikovaných rizik pokračování [autor]*

| Číslo rizika | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FMEA | X | | | | | | X | X | X | | X | X | | | |
| CARVER | | X | X | | X | X | X | X | X | | X | X | X | X | X |
| **Vyhodnocení** | | | | | | | X | X | X | | X | X | | | |

# 10 NÁVRH MINIMÁLNÍCH POŽADAVKŮ KYBERNETICKÉ OCHRANY RETAILU

Cílem této kapitoly je návrh minimálních požadavků pro zajištění ochrany před kybernetickými útoky se zaměřením na prostředí maloobchodu. Vstupními daty pro návrh těchto požadavků jsou nejzásadnější identifikovaná rizika vyplývající z provedených analýz předešlé kapitoly, přesněji jde o kategorie rizik: útoky z vnější sítě, chyby vnitřní sítě a softwaru, selhání přídavné funkce a rizika pochybení zaměstnance.

Prvním a zásadním požadavkem bez ohledu na předešlé analýzy je zpracování pravidel a směrnic fungování činností v organizaci prostřednictvím bezpečnostní politiky. Pro maximální účinnost bezpečnosti je nezbytně nutné mít stručný a jasně definovaný soubor pravidel, který musí být k dispozici všem zaměstnancům. Bezpečnostní politika musí být chráněna i před neoprávněným přístupem, pomocí kterého by útočník mohl získat náhled do vnitřního fungování společnosti. Nedostatečně zpracovaná bezpečnostní politika může také vést k úspěšným kybernetickým či jiným druhům útoků. Tento požadavek bych označil za základ a měl by být dodržován všemi podniky bez výjimky.

## 10.1 Útoky z vnější sítě

**Minimalizace rizik**: sociální inženýrství – infikování sítě maloobchodu malwarem, sociální inženýrství – únik citlivých informací

**Popis**: Pro vytvoření ochrany proti útokům sociálního inženýrství je zásadní implementace řady digitálních ochranných služeb a softwarových nástrojů. Veškerá zařízení podniku by měla být opatřena pravidelně aktualizovaným a udržovaným softwarem – anti-virem či anti-malwarem. Společnosti vyvíjející tyto druhy bezpečnostních softwarů se specializují nejen na osobní zařízení, ale i na sítě celých podniků, kde jsou schopni vytvořit opatření správně a na míru. Jedná se o softwary společností např. Avast, Eset, Norton, AVG a další. Doporučil bych i zvážení implementace speciálních algoritmů, které dokážou monitorovat chování systému a rozlišovat mezi legitimními a nelegitimními akcemi zaměstnanců. Tyto monitorující algoritmy používají strojové učení a stávají se velmi efektivními pro detekci a zastavení útoků sociálního inženýrství.

Jelikož sociální inženýrství cílí hlavně na lidské zaváhání, tou nejúčinnější strategií stále zůstává vzdělávání zaměstnanců prostřednictvím školení. Proto doporučuji pravidelné a systematické trénování všech zaměstnanců nejen ve směru povědomí o těchto hrozbách,

ale i v nutnosti zůstat ve střehu vůči podezřelým situacím. Pro zaměstnance je zásadní pochopení významu ochrany citlivých informací a získání představy toho, jakou podobu a dopad mohou skutečné útoky sociálního inženýrství mít.

Po uplatnění dostatečných bezpečnostních opatření doporučuji provádění občasných profesionálních penetračních testů v podobě malwaru nebo sociálního inženýrství, jejichž účelem bude zjištění pochybení zaměstnance, nebo technických slabin používaných sítí, systémů či aplikací.

**Minimalizace rizika**: Útok nultého dne

**Popis:** Jelikož se jedná o druh útoku, který využívá neznámou slabinu v systému, může být velmi obtížné se proti němu bránit. Avšak existují metody, které snižují šanci a dopad útoku, proto je řadím do minimálních požadavků ochrany. Pro nejvyšší možné zabezpečení navrhuji udržovat stálou aktuálnost všech systémů, zahrnující instalaci nejnovějších funkcí, aktualizaci všech ovladačů, ale i odstranění nepoužívaných softwarů. Doporučuji i metody ověřování vstupních dat, jak vytvořených zaměstnancem, tak dodaných z vnější sítě. Tyto metody jsou vykonávány firewally, jež chrání podniky prostřednictvím procesu skenování zranitelností a následné opravy potenciálních chyb. V případě maloobchodních společností využívajících on-line obchodování navrhuji použití firewallu pro webové aplikace, který je nasazen mezi samotnou aplikací a koncovým klientem, kde kontroluje příchozí provoz a filtruje škodlivé vstupy, které by mohly negativně ovlivnit chod systému.

**Minimalizace rizika**: Útok DDoS

**Popis:** Základním předpokladem pro zmírnění dopadu potencionálního DDoS útoku je poznat, kdy je podnik zasažen. To znamená, že je třeba implementovat technologii, která umožňuje monitorovat průměrné využití sítě v reálném čase a zároveň detekovat případné výkyvy či anomálie. Opět bych doporučil údržbu aktualizovaných a správně nakonfigurovaných firewallů včetně dalších programů sloužících k zabezpečení sítě. Mezi minimální požadavky vůči DDoS útoku řadím vyhotovený strategický plán reakce pro minimalizaci dopadu, který by měl obsahovat seznam všech nástrojů používaných pro detekci, hodnocení a filtrování útoku. Dále sestavený tým odborníků s jasně definovanými rolemi a pravidly popisující, jak postupovat, koho upozornit apod.

S rostoucí velikostí maloobchodních podniků roste šance DDoS útoků. Právě z toho důvodu bych větším společnostem doporučil kontaktovat profesionální poskytovatele služeb, kteří dokážou chránit aktiva pomocí přesměrování toku dat a tím snížit sílu útoku.

## 10.2 Chyby vnitřní sítě

**Minimalizace rizika:** Nezabezpečení systému firewallem

**Popis**: Brána firewall funguje zjednodušeně jako vrátný systému. Sleduje veškeré pokusy o získání přístupu a zároveň blokuje nežádoucí provoz nebo nerozpoznané zdroje. Absence či pouhá deaktivace brány firewall je pro systém maloobchodního či jiného podniku naprosto nepřijatelná. Je to základním prvkem kybernetické ochrany, který slouží jako filtr mezi vnitřní sítí a vnější sítí (internet). Rozhodně bych doporučil detailnější zaměření na konfiguraci firewallu a nastavení automatických aktualizací. Pro výběr typu firewallu bych do minimálních požadavků zařadil firewall nové generace (NGFW). Kromě tradičních funkcí firewallu dokáže např. blokovat moderní kybernetické hrozby, komunikovat a fungovat s ostatními bezpečnostními prvky architektury sítě nebo třeba chránit cloudové funkce (např. zálohování) jakožto virtuální firewall.

**Minimalizace rizika:** Slabé zabezpečení sítě Wi-Fi

**Popis**: Potřeba a pohodlí sítě Wi-Fi pro zaměstnance či pro zákazníky na prodejnách je v dnešní době již základní služba většiny maloobchodů. Avšak mnoho malých a středních podniků postrádá potřebné zdroje k řádnému zabezpečení jejich sítě, což ponechává podnik zranitelný vůči útočníkům, kteří se mohou pokusit ukrást firemní data či informace o zákaznících.

Základním opatřením by mělo být uložení routeru či směrovače na bezpečné místo s omezeným přístupem, např. v uzamčené skříni. V případě, že je Wi-Fi síť neveřejná, je potřeba nastavit silné přístupové heslo. Dalším velmi důležitým prvkem opatření je pravidelná kontrola, zda je směrovač aktualizován, neboť tyto aktualizace slouží k opravě nově zjištěných konkrétních chyb.

Minimálním požadavkem je taktéž implementace šifrovacího protokolu WPA2, který je označován jako dnešní standard. Avšak i tento protokol se podařilo prolomit a již nevykazuje takovou bezpečnost. Proto bych do požadavků dnešní doby zařadil i směrovače se šifrovacím protokolem WPA3.

## 10.3 Selhání přídavné funkce

**Minimalizace rizika:** Absence bezpečnostních certifikátů e-shopu, absence monitorování provozu IS/IT

**Popis**: Jako minimální požadavek pro zabezpečení webových stránek on-line obchodu navrhuji využití šifrovacího protokolu HTTPS. K vytvoření tohoto typu zabezpečení se na webový

server nainstaluje digitální certifikát TLS/SSL, který slouží k šifrování přenášených dat (tj. čísla kreditních karet, přihlašovací údaje). Dalším důležitým prvkem je ověření identity webových stránek, což zaručuje zákazníkům bezpečnou návštěvu e-shopu.

Pro získání certifikátů TLS/SSL je třeba kontaktovat certifikační organizaci, která poskytuje ověření identit a legitimit subjektů žádajících o certifikát. Aktuálně nejvíce používané certifikáty v České republice jsou Rapid SSL, Comodo nebo třeba GeoTrust.

Pro monitorování síťového provozu doporučuji využití systému detekce narušení (zkratkou IDS), jehož snahou je odhalit neobvyklé aktivity, které by mohly vést k narušení bezpečnosti počítačové sítě. Pro zvýšení bezpečnosti při monitorování navrhuji využití i systému prevence průniku (zkratkou IPS), jež dokáže navíc i aktivně blokovat a filtrovat detekovaný nežádoucí provoz na síti. U obou systémů je však velmi důležité dbát na správnost implementace a údržby.

Do nezbytných prvků monitorování provozu IS/IT je třeba zařadit i kontrolu logů, která by měla být implementována v celé síti včetně všech používaných síťových zařízení.

**Minimalizace rizika:** Nedostatečné zabezpečení cloudu maloobchodního systému

**Popis**: Pokud maloobchodní společnost využívá cloudových funkcí, stává se nejvyšší prioritou zabezpečení přístupu ke cloudovým datům a bezpečnost jejich ukládání. Zásadní je tedy ochrana všech údajů, které mohou zahrnovat citlivé informace o financích společnosti, obchodní tajemství či údaje o klientech.

Možná nejdůležitějším požadavkem pro minimalizaci tohoto rizika je výběr správného poskytovatele. Doporučil bych průzkum trhu a zjištění si co nejvíce informací o existujících možnostech. Správný poskytovatel je takový, který se dokáže přizpůsobit a navrhnout cloudový systém přímo na míru uživatele. Poskytovatel dále musí mít zpracovaný a dobře zdokumentovaný plán obrany pro zmírnění potencionálního útoku. Musí disponovat přísnými zásadami zabezpečení a zárukami zálohování.

Doporučil bych i určit si interní osobu, která bude zodpovědná za dokumentování všech ukládaných důvěrných informací do cloudového systému. Rizika narušení dat spolu s pokyny pro používání cloudu a přístupu k důvěrným informacím či výběru hesla by měli být plně pokryty důkladným školením zaměstnanců.

## 10.4 Pochybení zaměstnance

**Minimalizace rizik:** Vědomé prozrazení citlivých informací, nevědomé prozrazení citlivých informací, slabé heslo zaměstnance, nedostatečná kvalifikovanost zaměstnance

**Popis**: Hlavním požadavkem je rozhodně výběr správných zaměstnanců. Důkladný náborový proces musí zajistit, že je přijímaný zaměstnanec bude dostatečně spolehlivý. Náborový proces by se tak měl skládat z komplexní kontroly referencí zájemce a následného prověření pohovorem. Dále s ohledem na sdílení informací je rozumné zvážit, kdo získá dané informace a proč. Je třeba provádět i pravidelné školení zaměstnanců, zaměřené na práci s informacemi a zařízeními.

Podle zákona musí být implementován systém nástrojů pro ověření identit, které např. slouží k ověření identity uživatele před zahájením činnosti nebo řízení počtu možných neúspěšných pokusů o přihlášení. Do minimálních požadavků v tomto odvětví řadím použití vícefázového mechanismu pro přihlašování. Zaměstnanci by měli být poučeni o důležitosti tohoto mechanismu a výběru silných přihlašovacích hesel.

Důležité je i seznámení zaměstnanců s režimovými pravidly na pracovišti, patří tam například režim opuštění pracoviště řešené pomocí uzamknutí počítačového systému nebo zákaz používání soukromých přenosných datových nosičů (CD, flash disk apod.). Doporučil bych i zavedení omezení instalace neznámých softwarů či aplikací.

Pokud dojde k úniku, kompromitaci nebo ztrátě dat, každý zaměstnanec musí být poučen o povinnosti neprodleně ohlásit incident nadřízenému zaměstnanci.

# 11 ZÁVĚR

Úvodní část práce se zabývala právními předpisy a technickými normami, které souvisí s problematikou oblasti kybernetické a informační bezpečnosti.

Čtvrtá kapitola se věnovala definici a struktuře kyberprostoru včetně komplexního popisu jednotlivých vrstev, ze kterých je kyberprostor složen.

V páté kapitole byla představena a definována kybernetická bezpečnost, která byla doplněna o princip informační bezpečnosti. Kapitola shrnula jednotlivé prvky tvořící základ informační bezpečnosti a rozebrala běžně zpracovávané typy dat a informací v organizacích.

Šestá kapitola se zabývala klasifikací kybernetických hrozeb a detailním popisem jednotlivých typů kybernetických útoků.

Sedmá kapitola se zaměřila na deskripci procesů včetně charakteristiky podpůrných informačních systémů a technologií maloobchodu, konkrétně byly představeny front-office a back-office systémy. Další části kapitoly se věnovaly způsobům fungování elektronického obchodu a způsobům zabezpečení.

V osmé kapitole byly komplexně shrnuty jednotlivé technické prostředky a nástroje, které v současné době slouží jako bezpečnostní standard kybernetické ochrany.

V deváté kapitole byla posouzena bezpečnostní rizika související s napadení informačního systému oblasti maloobchodu. Pro identifikaci rizik byla z důvodu přehledného grafického zobrazení příčin a následku zvolena metoda Ishikawova diagramu. Následné posouzení rizik proběhlo pomocí analytických metod FMEA a CARVER doplněných o Paretův princip. V poslední části kapitoly proběhla vzájemná komparace výsledků obou zpracovaných metod.

Závěrečná část práce byla věnována návrhu minimálních požadavků kybernetické ochrany se zaměřením na prostředí maloobchodu, kdy byla navržena vhodná opatření pro minimalizaci nejvýznamnějších identifikovaných rizik vyplývajících z předešlé kapitoly.

Cílem této práce byla studie kybernetické ochrany a návrh minimálních požadavků pro zajištění ochrany před kybernetickými útoky se zaměřením na prostředí retailu. Byla provedena analýza procesů v maloobchodu a deskripce kybernetických útoků, technických prostředků a technologií pro ochranu před kybernetickými útoky. Za využití analytických metod bylo provedeno posouzení bezpečnostních rizik informačních systémů retailu a následně byl proveden návrh minimálních požadavků kybernetické ochrany.

# SEZNAM POUŽITÉ LITERATURY

## Monografie


[1] CIMLER, Petr a Dana ZADRAŽILOVÁ. *Retail management*. Praha: Management Press, 2007. ISBN 978-80-7261-167-6.

[2] KOLOUCH Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016. 522 stran. ISBN:978-80-88168-15-7

[3] PARKER, Donn B. *Fighting Computer Crime: A New Framework for Protecting Information*. New York, NY, 1998. ISBN 0-471-16378-3.

[4] SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

[5] ŠČUREK, Radomír. *Studie analýzy rizika protiprávních činů na letišti*. Skriptum, VŠB-TU Ostrava: Ostrava 2009, 115 str.

[6] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk s.r.o., 2018. ISBN 978-80-7380-737-5.


## Právní předpisy a normy


[7] ČSN EN 60812. Techniky analýzy bezporuchovosti systémů – Postup analýzy způsobů a důsledků poruch (FMEA). Praha: Český normalizační institut, 2007. 44 s. Třídící znak 010675

[8] ČSN ISO/IEC 27001:2014 informační technologie – bezpečnostní techniky – systémy managementu bezpečnosti informací – požadavky. Praha: Český normalizační institut, 2014. 28s. Třídící znak: 369797

[9] ČSN ISO/IEC 27002:2014 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Praha: Český normalizační institut, 2014. Třídící znak: 369798

[10] Nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016

[11] Vyhláška č. 82/2018 Sb., ze dne 21. května 2018

## Elektronické zdroje


[12] ANDREWS, Stuart. *Dark Side of the Web: „The Surface Web"* [online]. 2012 [cit. 2020-11-27]. Dostupné z: https://davidenewmedia.wordpress.com/workingterms/the-surface-web/

[13] BERGMAN, Michael K. *The Deep Web: „Surfacing Hidden Value"* [online]. 2001, [cit. 2020-11-27]. Dostupné z: https://quod.lib.umich.edu/cgi/t/text/textidx?c=jep;view=text;rgn=main;idno=3336451.0007.104

[14] CISCO. *What Are the Most Common Cyber Attacks?* Cisco Systems [online]. 2020 [cit. 2021-01-07]. Dostupné z: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

[15] CLOUDFLARE. *What is HTTPS*? CloudFlare [online]. 2021 [cit. 2021-02-27]. Dostupné z: https://www.cloudflare.com/learning/ssl/what-is-https/

[16] CLOUDFLARE. *What is SSL?* CloudFlare [online]. 2021 [cit. 2021-02-27]. Dostupné z: https://www.cloudflare.com/learning/ssl/what-is-ssl/

[17] CRAIGEN, D., DIAKUN-THIBAULT, N., PURSE, R. *Defining Cybersecurity.* [online]. 2014. [cit. 2020-11-27]. Dostupné z: http://doi.org/10.22215/timreview/835

[18] EMERCHANTPAY. *What is a payment gateway and how does it work?* Emerchantpay [online]. 2019 [cit. 2021-02-27]. Dostupné z: https://www.emerchantpay.com/insights/what-is-a-payment-gateway-and-how-does-it-work/

[19] ESET. *Firewall*. Eset [online]. 2020 [cit. 2021-02-27]. Dostupné z: https://www.eset.com/cz/firewall/

[20] FEDERATION OF AMERICAN SCIENTISTS. *Target Analysis Process (CARVER).* Federation of American Scientists [online]. [cit. 2021-03-15]. Dostupné z: https://fas.org/irp/doddir/army/fm34-36/appd.htm

[21] FRUHLINGER, Josh. *DDoS explained: How distributed denial of service attacks are evolving.* CSO [online]. 2021 [cit. 2021-02-15]. Dostupné z: https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html

[22] GONZALEZ, CYNTHIA. *Top 5 Social Engineering Techniques and How to Prevent Them.* Exabeam [online]. 2020 [cit. 2021-02-15]. Dostupné z: https://www.exabeam.com/information-security/social-engineering/

[23] GRIMES, Roger. *9 types of malware and how to recognize them*. CSO [online]. 2020 [cit. 2021-02-15]. Dostupné z: https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html

[24] HICKS, Kristen. *What are Online Payment Methods?* HostGator [online]. 2019 [cit. 2021-02-27]. Dostupné z: https://www.hostgator.com/blog/online-payment-methods-ecommerce/

[25] CHIVERS, Kyle. *Zero-day vulnerability: What it is, and how it works.* Norton [online]. 2019 [cit. 2021-03-21]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

[26] IMPERVA. *Social Engineering*. Imperva [online]. [cit. 2021-02-15]. Dostupné z: https://www.imperva.com/learn/application-security/social-engineering-attack/

[27] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. Praha 2013, [cit. 2020-11-27]. Dostupné z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

[28] JIRÁSEK, Petr. *Kybernetická bezpečnost (Cyber Security)* [online]. 1.11.2017, [cit. 2020-11-27]. Dostupné z: https://www.cybersecurity.cz/basic.html

[29] KRUCEK. *Penetrační testování: Co je penetrační testování a jaký má účel.* Krucek [online]. 2021 [cit. 2021-02-27]. Dostupné z: https://www.krucek.cz/audit/penetracni-testovani/

[30] LEXICO, *Cybersecurity*. [online]. 2020 Oxford Online Dictionary. [cit. 2020-11-27]. Dostupné z: https://en.oxforddictionaries.com/definition/cybersecurity

[31] LOSHIN, Peter a Michael COBB. *Encryption technology: Co je penetrační testování a jaký má účel*. TechTarget [online]. 2020 [cit. 2021-02-27]. Dostupné z: https://searchsecurity.techtarget.com/definition/encryption

[32] MANAGEMENTMANIA. *Ishikawův diagram.* Management Mania [online]. 2015 [cit. 2021-03-21]. Dostupné z: https://managementmania.com/cs/ishikawuv-diagram

[33] MARKS, Paul. *Cybersecurity and the Parkerian Hexad.* [online]. 2019, [cit. 2020-11-27]. Dostupné z: https://www.staffhosteurope.com/blog/2019/03/cybersecurity-and-the-parkerian-hexad

[34] MELNICK, Jeff. *Top 10 Most Common Types of Cyber Attacks.* Netwrix [online]. 2018 [cit. 2021-02-15]. Dostupné z: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Malware%20attack

[35] MERICHOVITIS, Christos. *Everything about eCommerce and eShops.* Devseg [online]. 2019 [cit. 2021-02-27]. Dostupné z: https://devseg.com/ecommerce-and-eshops/

[36] NOVÁK, Luděk a Josef POŽÁR. *Systém řízení informační bezpečnosti* [online]. 2011 [cit. 2021-02-15]. ISBN ISBN 978-80-7251-356-7. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf

[37] PCI SECURITY STANDARDS COUNCIL, LLC. *Payment Card Industry (PCI): Card Production and Provisioning* [online]. PCI Security Standards Council, 2016 [cit. 2021-03-31]. Dostupné z: https://www.pcisecuritystandards.org/documents/PCI_Card_Production_Logical_Security_Requirements_v2_Nov2016.pdf?agreement=true&time=1484176101208

[38] PENDER-BEY, Georgie. *THE PARKERIAN HEXAD*: *The CIA Triad Model Expanded* [online]. 2012 [cit. 2020-11-27]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

[39] POINTOFSALE. *Point of Sale Systems Explained: What is a POS System?* Point of Sale [online]. 2019 [cit. 2021-02-04]. Dostupné z: https://pointofsale.com/point-of-sale-systems-explained-what-is-a-pos-system/

[40] PRACHAŘ, Jan. *Teorie obchodu* [online]. Kunovice: Evropský polytechnický institut. 2011 [cit. 2021-01-07]. ISBN 978-80-7314-262-9. Dostupné z: https://docplayer.cz/4510668-Evropsky-polytechnicky-institut-s-r-o-1-soukroma-vysoka-skola-na-morave-kunovice-teorie-obchodu-ing-jan-prachar-ph-d.html

[41] PRIMASELLER. *The Complete Guide To POS: Point Of Sale, POS Systems, POS Terminals And More*. PrimaSeller [online]. [cit. 2021-02-04]. Dostupné z: https://www.primaseller.com/knowledge-base/what-is-pos-point-of-sale/

[42] SHEA, Sharon. *How to prevent network eavesdropping attacks*. TechTarget [online]. 2020 [cit. 2021-03-21]. Dostupné z: https://searchsecurity.techtarget.com/answer/How-to-prevent-network-sniffing-and-eavesdropping

[43] SOLMS, Rossouw von, NIEKERK, Johan van. *Computers & Security* [online]. 2013, [cit. 2020-11-27]. Dostupné z: https://profsandhu.com/cs6393_s19/Solms-Niekerk-2013.pdf

[44] TECHOPEDIA. *Back Office Application: What does Back Office Application mean?* Techopedia [online]. 2012 [cit. 2021-02-08]. Dostupné z: https://www.techopedia.com/definition/1406/back-office-application

[45] TUNGGAL, Abi Tyas. *What is a Cyber Threat?* Upguard [online]. 2020 [cit. 2021-01-07]. Dostupné z: https://www.upguard.com/blog/cyber-threat

[46] VANE, Michael. *Cyberspace Operations Concept Capability Plan 2016-2028* [online]. 2010, [cit. 2020-11-27]. Dostupné z: Cyberspace Operations Concept Capability Plan 2016-2028, 20 Feb 2010

[47] WIKISOFIA. *Isms*. Wikisofia [online] 2013. [cit. 2021-02-15]. Dostupné z: https://wikisofia.cz/wiki/ISMS

[48] WOODFORD, Chris. *E-commerce: How e-commerce works.* ExplainThatStuff [online]. 2021 [cit. 2021-02-27]. Dostupné z: https://www.explainthatstuff.com/ecommerce.html

[49] ZIMMERMAN, Ann. *Check Out the Future of Shopping.* The Wall Street Journal [online]. 2011 [cit. 2021-02-05]. Dostupné z: https://www.wsj.com/articles/SB10001424052748703421204576329253050637400

# SEZNAM OBRÁZKŮ

# SEZNAM TABULEK

# SEZNAM PŘÍLOH